* Geometric control of modular Jacobians

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

Talk on March 26, 2015 (Cambridge, England).

See www.math.ucla.edu/~hida/LTS.pdf

*The author is partially supported by the NSF grant: DMS 0753991.

Analyzing known elementary relations between $U(p)$ operators and Picard functoriality of the Jacobians of each tower of modular curves of p-power level, we get fairly exact control of the ordinary part of the limit Barsotti-Tate groups and the (p-adically completed) limit Mordell-Weil groups with respect to the weight Iwasawa algebra. Computing Galois cohomology of these controlled Galois modules, we hope to get good control of the (ordinary part of) limit Selmer groups and limit Tate-Shafarevich groups.

§0. Exotic Γ_1-type congruence subgroups:

Let $\Gamma := \mathbb{Z}_p^\times/\mu_{p-1} \cong 1 + p\mathbb{Z}_p$, for a prime $p \geq 5$. Fix an exact sequence of profinite groups $1 \to H_p \to \Gamma \times \Gamma \xrightarrow{\pi_\Gamma} \Gamma \to 1$, and regard H_p as a subgroup of $\Gamma \times \Gamma$. This implies $\pi_\Gamma(a,d) = a^\alpha d^{-\delta}$ for a pair $(\alpha, \delta) \in \mathbb{Z}_p^2$ with $\alpha\mathbb{Z}_p + \delta\mathbb{Z}_p = \mathbb{Z}_p$. Let H be the pull-back of H_p to $\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$. Define, for $\widehat{\mathbb{Z}} = \prod_{l:\text{primes}} \mathbb{Z}_l$ and $0 < M, N \in \mathbb{Z}$,

$$\widehat{\Gamma}_0(M) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \middle| c \in M\widehat{\mathbb{Z}} \right\},$$
$$\widehat{\Gamma}_1(M) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(M) \middle| d - 1 \in M\widehat{\mathbb{Z}} \right\},$$
$$\widehat{\Gamma}_1^1(M) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(M) \middle| a - 1 \in M\widehat{\mathbb{Z}} \right\},$$
$$\widehat{\Gamma}_s = \widehat{\Gamma}_{H,s} := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \widehat{\Gamma}_0(p^s) \cap \widehat{\Gamma}_1(N) \middle| (a_p, d_p) \in H/H_p^{p^{s-1}} \right\}$$
$$\widehat{\Gamma}_s^r = \widehat{\Gamma}_{H,s}^r := \widehat{\Gamma}_0(p^s) \cap \widehat{\Gamma}_r \quad (s \geq r,\ p \nmid N).$$

The group $\Gamma_r := \widehat{\Gamma}_r \cap \mathrm{SL}_2(\mathbb{Q})$ is independent of H almost $\Gamma_1(Np^r)$.

§1. Exotic modular tower.

Let $X_{r/\mathbb{Q}}$ and $X^r_{s/\mathbb{Q}}$ be Shimura's canonical models associated with $\widehat{\Gamma}_r$ and $\widehat{\Gamma}^r_s$. They are geometrically connected curve canonically defined over $\mathbb{Q}$ and the moduli of elliptic curves with certain level structure (which can be defined over $\mathbb{Z}_{(p)}$).

We have an adelic expression of their complex points.

$$X^r_s(\mathbb{C}) = \mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A})/\widehat{\Gamma}^r_s\mathbb{R}^\times_+\mathrm{SO}_2(\mathbb{R}) \cong \Gamma^r_s\backslash\mathfrak{H},$$

where $\Gamma^r_s = \widehat{\Gamma}^r_s \cap \mathrm{SL}_2(\mathbb{Q})$ and $\Gamma_r = \widehat{\Gamma}_r \cap \mathrm{SL}_2(\mathbb{Q})$. Note that Γ_r and Γ^r_s is independent of the choice of (α, δ).

Write $J^r_{s/\mathbb{Q}}$ and $J_{r/\mathbb{Q}}$ for the corresponding Jacobian varieties.

§2. Galois representation.

Let $f \in S_2(\Gamma_r)$ be a Hecke eigenform and ρ_f be its p-adic Galois representation, taking the choice $(\alpha,\delta) = (0,1)$. Note that $\det \rho_f = \nu\psi_f$ for a p-power order character ψ which has a unique square root $\sqrt{\psi_f}$ of p-power order. Then the same f gives rise to $\rho_f \otimes \sqrt{\psi_f}^{-1}$ if $(\alpha,\delta) = (1,1)$ and we regard $f dz \in H^0(X_r, \Omega_{X_r/\mathbb{C}})$.

If we write the Mazur-Kitagawa p-adic L-function (interpolating $L(s,f)$) for f in a two variable nearly ordinary family as $L(k,s)$ for the weight variable $k \leftrightarrow f$ and the cyclotomic variable s, the tower $\{X_r\}_r$ for (α,δ) gives the one variable variation the one variable p-adic L-function $k \mapsto L(2\delta k + 2, \alpha k + 1)$. In particular, if $(\alpha,\delta) = (0,1)$ gives the ordinary variation: the one variable p-adic L-function $k \mapsto L(2k+2,1)$, and $(\alpha,\delta) = (1,1)$ gives the central critical variation: the one variable p-adic L-function $k \mapsto L(2k+2,k+1)$ (which can be identically 0).

§3. Ordinary Λ-BT group.

Define $\mathcal{G} = \mathcal{G}_{\alpha,\delta} := \varinjlim_s J_s[p^\infty]^{\mathrm{ord}}$ sometimes over $\mathbb{Q}$ sometimes over $\mathbb{Z}_{(p)}[\mu_{p^\infty}]$. Here "ord" indicates the image of the idempotent $e := \varinjlim_n U(p)^{n!}$. Since $\Gamma = (\Gamma \times \Gamma)/H = \varprojlim_s \widehat{\Gamma}_s/\widehat{\Gamma}_s^1$ naturally acts on $\mathcal{G}$, $\mathcal{G}$ has natural action of the weight Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\Gamma]] = \mathbb{Z}_p[[T]]$ with $t = 1 + T$ generating Γ.

The Λ-BT group $\mathcal{G}$ satisfies

(CT) For $\mathcal{G}_s := J_s[p^\infty]^{\mathrm{ord}}$, we have

$$\mathcal{G}_s = \mathcal{G}[t^{p^{s-1}} - 1] := \mathrm{Ker}(t^{p^{s-1}} - 1 : \mathcal{G} \to \mathcal{G})$$

(in particular, $\mathcal{G}_{s/R} \hookrightarrow \mathcal{G}_{/R}$ is a closed immersion for $R = \mathbb{Z}_{(p)}[\mu_{p^\infty}]$);

(DV) The geometric generic fiber $\mathcal{G}(\overline{K})$ is isomorphic to $(\Lambda^*)^n$ for the Pontryagin dual $\Lambda^\vee := \mathrm{Hom}_{\mathbb{Z}_p}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p)$; so, $T\mathcal{G} = \mathrm{Hom}_\Lambda(\Lambda^\vee, \mathcal{G}(\overline{K}))$ is Λ-free of finite rank.

§4. The $U(p)$-operators.

Since $\Gamma_s^r \triangleright \Gamma_s$, consider the cyclic quotient group $C := \frac{\Gamma_s^r}{\Gamma_s}$ of order p^{s-r}. By the inflation restriction sequence, we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} H^1(C,\mathbf{T}) & \stackrel{\hookrightarrow}{\longrightarrow} & H^1(\Gamma_s^r,\mathbf{T}) & \longrightarrow & H^1(\Gamma_s,\mathbf{T})^{\gamma^{p^r}=1} & \longrightarrow & H^2(C,\mathbf{T})=0 \\ \uparrow & & \cup\uparrow & & \uparrow\cup & & \uparrow \\ ? & \longrightarrow & J_s^r(\mathbb{C}) & \longrightarrow & J_s(\mathbb{C})[\gamma^{p^{r-1}}-1] & \longrightarrow & ?. \end{array}$$

Since C is a finite cyclic group of order p^{s-r} (with generator g) acting trivially on $\mathbf{T}$, we have $H^1(C,\mathbf{T}) = \mathrm{Hom}(C,\mathbf{T}) \cong C$ and

$$H^2(C,\mathbf{T}) = \mathbf{T}/(1+g+\cdots+g^{p^{s-r}-1}) = \mathbf{T}/p^{s-r}\mathbf{T} = 0.$$

§**5. The $U(p)$-isomorphism.** By a cocycle computation, we confirm that $U(p)$ acts on $H^1(C, \mathbf{T})$ via multiplication by its degree p, and hence $U(p)^{s-r}$ kill $H^1(C, \mathbf{T})$.
Hence $J_s^r \to J_s$ is an $U(p)$-isomorphism over $\mathbb{C}$ (meaning its kernel and cokernel are killed by a power of $U(p)$) and hence over $\mathbb{Q}$. We record what we have proven:

$$U(p)^{s-r}(H^1(C, \mathbf{T})) = H^2(C, \mathbf{T}) = 0.$$

This fact has been exploited by the speaker to show (CT) and (DV).

By (DV), for any factor $\varpi | t^{p^s} - 1$, we have an exact sequence

$$0 \to \mathcal{G}[\varpi] \to \mathcal{G} \xrightarrow{\varpi} \mathcal{G} \to 0 \text{ (the first fundamental sequence)}$$

of fppf abelian sheaves.

§6. The $U(p)$-identity.

Note a simple identity:

$$U^s_r(p^{s-r}) := \Gamma^r_s \backslash \Gamma^r_s \begin{pmatrix} 1 & 0 \\ 0 & p^{s-r} \end{pmatrix} \Gamma_1(Np^r) = \left\{ \begin{pmatrix} 1 & u \\ 0 & p^{s-r} \end{pmatrix} \middle| u \mod p^{s-r} \right\}$$
$$= \Gamma_1(Np^r) \backslash \Gamma_1(Np^r) \begin{pmatrix} 1 & 0 \\ 0 & p^{s-r} \end{pmatrix} \Gamma_1(Np^r) =: U(p^{s-r})$$

which implies the relation of $U(p^{s-r})$-operators:

$$\begin{array}{ccc} J_{r/\mathbb{Q}} & \xrightarrow{\pi^*} & J^r_{s/\mathbb{Q}} \\ \downarrow u & \swarrow u' & \downarrow u'' \\ J_{r/\mathbb{Q}} & \xrightarrow{\pi^*} & J^r_{s/\mathbb{Q}}, \end{array}$$

where the middle u' is given by $U^s_r(p^{s-r})$ and u and u'' are $U(p^{s-r})$. Then the above diagram implies

$$J_{r/\mathbb{Q}}[p^\infty]^{\mathrm{ord}} \cong J^r_{s/\mathbb{Q}}[p^\infty]^{\mathrm{ord}}, \;\; J^{\mathrm{ord}}_{r/\mathbb{Q}} \cong J^{r,\mathrm{ord}}_{s/\mathbb{Q}}.$$

§7. Replace $H^1(X_s, \mathbf{T})$ by $H^1(X_s, O_{X_s}^\times)$.

Note $H^1_{\mathrm{fppf}}(X, O_{X/\mathbb{Q}}^\times) = \mathrm{Pic}_{X/\mathbb{Q}}$ for a smooth geometrically irreducible curve X. Thus we have the following commutative diagram with exact rows and columns for $X = X_s$ and $Y = X_s^r$:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathbb{Z} & = & \mathbb{Z} & \longrightarrow & 0 \\
\uparrow & & \mathrm{deg}\uparrow\mathrm{onto} & & \mathrm{deg}\uparrow\mathrm{onto} & & \uparrow \\
\check{H}^1(\underline{H}^0_Y) & \longrightarrow & \mathrm{Pic}_{Y/S}(T) & \xrightarrow{b} & \check{H}^0(\frac{X_T}{Y_T}, \mathrm{Pic}_{Y/S}(T)) & \longrightarrow & \check{H}^2(\underline{H}^0_Y) \\
\uparrow & & \cup\uparrow & & \uparrow\cup & & \uparrow \\
?_1 & \longrightarrow & J_Y(T) & \xrightarrow[c]{} & \check{H}^0(\frac{X_T}{Y_T}, J_X(T)) & \longrightarrow & ?_2,
\end{array}$$

Here $J_?$ is the Jacobian of the curve ?, and $\underline{H}^\bullet_Y := \underline{H}^\bullet(\mathbb{G}_{m/Y})(\mathcal{U}) = H^\bullet_{\mathrm{fppf}}(\mathcal{U}, O_{\mathcal{U}}^\times)$ for a Y-scheme $\mathcal{U}$ as a presheaf. By Čech cohomology computation, one can easily show $e(\check{H}^\bullet(\underline{H}^0_Y)) = 0$.

§8. Arithmetic points.

Define $\mathbf{h} = \mathbf{h}_{\alpha,\delta} := \Lambda[T(n)|n = 1, 2, \ldots] \subset \mathrm{End}_\Lambda(T\mathcal{G})$. Take a connected component Spec($\mathbb{T}$) and assume that $\mathbb{T}$ is a **unique factorization domain** (this is usually the case).

Define $\mathcal{A}_\mathbb{T}$ for the set of points in Spec($\mathbb{T}$)($\overline{\mathbb{Q}}_p$) with $P|(t^{p^r} - 1)$ for some $r > 0$. Then we have an abelian varieties $A_P \subset J_r$ and $J_r \twoheadrightarrow B_P$ associated to P and a Hecke eigenform f_P associated to P. Write $H_P = \mathbb{Q}(f_P) \subset \mathrm{End}(A_{P/\mathbb{Q}}) \otimes \mathbb{Q}$ for the Hecke field of f_P.

We then put

$$\Omega_\mathbb{T} = \{P \in \mathcal{A}_\mathbb{T} | A_P \text{ has potentially good reduction modulo } p\}.$$

§9. Second fundamental exact sequence

Define an fppf sheaf $J_s^{\mathrm{ord}}(R) := e(\varprojlim_n J_s(R) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z})$ and put $J_\infty^{\mathrm{ord}} := \varinjlim_s J_s^{\mathrm{ord}}$. Since $\mathbb{T}$ is a UFD, each prime $P \in \mathcal{A}_{\mathbb{T}}$ is generated by $\varpi \in \mathbb{T}$ associated to a Hecke eigenform $f_P \in S_2(\widehat{\Gamma}_r)$ and an abelian subvariety $A_P \subset J_r$ and an abelian quotient $J_r \twoheadrightarrow B_P$ isogenous to A_P. We get the following exact sequence of fppf sheaves:

$$0 \to A_P^{\mathrm{ord}} \to J_{\infty,\mathbb{T}}^{\mathrm{ord}} \xrightarrow{\varpi} J_{\infty,\mathbb{T}}^{\mathrm{ord}} \to B_P^{\mathrm{ord}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to 0,$$

where $X^{\mathrm{ord}}(R) = e(\varprojlim_n X(R) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z})$ for an abelian variety X and $J_{\infty,\mathbb{T}}^{\mathrm{ord}} = J_\infty^{\mathrm{ord}} \otimes_{\mathbf{h}} \mathbb{T}$. In other words, $A_P^{\mathrm{ord}} \cong J_{s,\mathbb{T}}^{\mathrm{ord}}[\varpi] = \mathrm{Ker}(\varpi : J_{s,\mathbb{T}}^{\mathrm{ord}} \to J_{s,\mathbb{T}}^{\mathrm{ord}})$ for all $s \geq r$ and $B_P^{\mathrm{ord}} \cong J_{r,\mathbb{T}}^{\mathrm{ord}}/\varpi(J_{r,\mathbb{T}}^{\mathrm{ord}})$, but the limit $\varinjlim_{s \geq r} J_{s,\mathbb{T}}^{\mathrm{ord}}/\varpi(J_{s,\mathbb{T}}^{\mathrm{ord}})$ is isomorphic to $B_P^{\mathrm{ord}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

§10. Arithmetic cohomology groups.

For a finite set of places S of a number field K containing all places above Np and ∞, write K^S/K for the maximal extension unramified outside S. For a topological $\mathrm{Gal}(K^S/K)$-module M and $v \in S$, we write $H^\bullet(K^S/K, M)$ (resp. $H^\bullet(K_v, M)$ for the v-completion K_v of K) for the continuous cohomology for the profinite group $\mathrm{Gal}(K^S/K)$ (resp. $\mathrm{Gal}(\overline{K}_v/K_v)$ for an algebraic closure $\overline{K}_v$ of K_v). Define

$$\underline{\mathrm{III}}(K^S/K, M) = \mathrm{Ker}(H^1(K^S/K, M) \to \prod_{v \in S} H^1(K_v, M)) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

In addition to the Mordell–Weil group $J_r(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$, we study the Tate–Shafarevich group $\underline{\mathrm{III}}_K(J_r^{\mathrm{ord}})$, $\underline{\mathrm{III}}_K(K^S/K, J_r[p^\infty]^{\mathrm{ord}})$ and the Selmer group

$$\mathrm{Sel}_K(J_r^{\mathrm{ord}}) = \mathrm{Ker}(H^1(K^S/K, J_r[p^\infty]^{\mathrm{ord}}) \to \prod_{v \in S} H^1(K_v, J_r^{\mathrm{ord}})).$$

§11. Theorem for Tate–Shafarevich groups.

Theorem III. *Suppose that $\mathbb{T}$ is a unique factorization domain.*

1. *If* $\underline{\underline{III}}_K(K^S/K, A_{P_0}[p^\infty]^{\text{ord}})$ *is finite for a single point* $P_0 \in \Omega_{\mathbb{T}}$, *then* $\underline{\underline{III}}_K(K^S/K, A_P[p^\infty]^{\text{ord}})$ *is finite for almost all* $P \in \Omega_{\mathbb{T}}$.

2. *If* $\underline{\underline{III}}_K(A_{P_0}^{\text{ord}})$ *is finite and* $\dim_{H_{P_0}} A_{P_0}(K) \otimes_{\mathbb{Z}} \mathbb{Q} \leq 1$ *for a single point* $P_0 \in \Omega_{\mathbb{T}}$, *then* $\underline{\underline{III}}_K(A_P^{\text{ord}})$ *is finite for almost all* $P \in \Omega_{\mathbb{T}}$.

3. *If* $|\underline{\underline{III}}_K(A_{P_0}^{\text{ord}})| < \infty$ *and* $\dim_{H_{P_0}} A_{P_0}(K) \otimes_{\mathbb{Z}} \mathbb{Q} \leq 1$ *for a single point* $P_0 \in \Omega_{\mathbb{T}}$, *then* $\dim_{H_P} A_P(K) \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ *or* 1 *independent of* P *for almost all* $P \in \Omega_{\mathbb{T}}$.

§12. Theorem for Selmer groups.

Theorem S. *Suppose that $\mathbb{T}$ is a unique factorization domain.*

1. *If* $\mathrm{Sel}_K(A^{\mathrm{ord}}_{P_0})$ *is finite for a single point* $P_0 \in \Omega_{\mathbb{T}}$*, then* $\mathrm{Sel}_K(A^{\mathrm{ord}}_{P})$ *is finite for almost all* $P \in \Omega_{\mathbb{T}}$*.*

2. *Suppose that all prime factors of* p *in* K *has residual degree* 1*. If* $\mathrm{Sel}_K(A^{\mathrm{ord}}_{P_0}) = 0$ *for a single point* $P_0 \in \Omega_{\mathbb{T}}$ *such that* $A_{P_0/\mathbb{Q}}$ *has good reduction modulo* p *with* $A_{P_0}(\mathbb{F}_p) = 0$*,* $\mathrm{Sel}_K(A^{\mathrm{ord}}_{P})$ *is finite for all* $P \in \Omega_{\mathbb{T}}$ *without exception.*

This type of control has been studied by other people, notably, J. Nekovar.

§13. Abelian variety of GL(2)-type.

A $\mathbb{Q}$-simple abelian variety (with a polarization) is "*of* GL(2)-*type*" if we have a subfield $H_A \subset \mathrm{End}^0(A_{/\mathbb{Q}}) = \mathrm{End}(A_{/\mathbb{Q}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ of degree $\dim A$ (stable under Rosati-involution).

Then, for the two-dimensional compatible system ρ_A of Galois representation of A with coefficients in H_A, H_A is generated by traces $\mathrm{Tr}(\rho_A(\mathrm{Frob}_l))$ of Frobenius elements Frob_l for primes l of good reduction (i.e., the field H_A is uniquely determined by A). We always regard $\mathbb{Q}$ as a subfield of the algebraic closure $\overline{\mathbb{Q}}$. Thus $O'_A := \mathrm{End}(A_{/\mathbb{Q}}) \cap H_A$ is an order of H_A. Write O_A for the integer ring of H_A. Replacing A by the abelian variety representing the group functor $R \mapsto A(R) \otimes_{O'_A} O_A$, we may choose A so that $O'_A = O_A$ in the $\mathbb{Q}$-isogeny class of A.

§14. Congruence among abelian varieties.

To reformulate the result, we introduce congruence among abelian varieties.

For two abelian varieties A and B of GL(2)-type over $\mathbb{Q}$, we say that A is *congruent to* B *modulo a prime* p *over* $\mathbb{Q}$ if we have a prime factor $\mathfrak{p}_A$ (resp. $\mathfrak{p}_B$) of p in O_A (reso. O_B) and field embeddings $\sigma_A : O_A/\mathfrak{p}_A \hookrightarrow \overline{\mathbb{F}}_p$ and $\sigma_B : O_B/\mathfrak{p}_B \hookrightarrow \overline{\mathbb{F}}_p$ such that $(A[\mathfrak{p}_A] \otimes_{O_A/\mathfrak{p}_A,\sigma_A} \overline{\mathbb{F}}_p)^{ss} \cong (B[\mathfrak{p}_B] \otimes_{O_B/\mathfrak{p}_B,\sigma_B} \overline{\mathbb{F}}_p)^{ss}$ as semi-simplified Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.

We call that A is of $\mathfrak{p}_A$-type (α, δ) if the $\mathfrak{p}_A$-adic Tate module produces a local representation $\rho_{\mathfrak{p}_A}$ of Gal$(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $\rho_{\mathfrak{p}_A}|_{I_p} \cong \begin{pmatrix} \nu_p\epsilon^{-\delta} & * \\ 0 & \epsilon^{\alpha} \end{pmatrix}$ for a character $\epsilon : I_p \to \mu_{p^\infty}$ of the inertia group I_p at p.

§15. Rational elliptic curves.

Let $E_{/\mathbb{Q}}$ be an elliptic curve. Writing the Hasse–Weil L-function $L(s,E)$ as a Dirichlet series $\sum_{n=1} a_n n^{-s}$ ($a_n \in \mathbb{Z}$) (i.e., $1+p-a_p = |E(\mathbb{F}_p)|$ for each prime p of good reduction for E), we call p *admissible* for E if E has good reduction at p and (a_p mod p) is not in $\Omega_E := \{\pm 1, 0\}$ (so, 2 and 3 are not admissible). Therefore, the maximal étale quotient of $E[p]$ over $\mathbb{Z}_p$ is **not** isomorphic to $\mathbb{Z}/p\mathbb{Z}$ up to unramified quadratic twists.

By the Hasse bound $|a_p| \leq 2\sqrt{p}$, $p \geq 7$ is not admissible if and only if $a_p \in \Omega_E$. Thus if E does not have complex multiplication, the Dirichlet density of non-admissible primes is zero by a theorem of Serre as $L(s,E) = L(s,f)$ for a rational Hecke eigenform f.

§16. Vanishing of $\underline{\text{III}}$ proliferates.

Let $E_{/\mathbb{Q}}$ be an elliptic curve with $|\underline{\text{III}}_K(E)| < \infty$ and $\dim_{\mathbb{Q}} E(K) \otimes_{\mathbb{Z}} \mathbb{Q} \leq 1$. Let N be the conductor of E, and pick an admissible prime p for E. Consider the set $\mathcal{A}_{E,p}$ made up of all $\mathbb{Q}$-isogeny classes of $\mathbb{Q}$-simple abelian varieties $A_{/\mathbb{Q}}$ of $\mathfrak{p}_A$-type (α, δ) with prime-to-p conductor N congruent to E modulo p over $\mathbb{Q}$.

Theorem B. *There exists an explicit (computable) finite set S_E of primes depending on N but independent of K such that if $p \notin S_E$, almost all members $A \in \mathcal{A}_{E,p}$ have finite $\underline{III}_K(A)[\mathfrak{p}_A^\infty]$ and constant dimension $\dim_{H_A} A(K) \leq 1$. If further $E(K)_p = \underline{III}_K(E) = 0$ (i.e., $\mathrm{Sel}_K(E) = 0$ in short) and E can be embedded into J_r for some $r > 0$, then as long as p totally splits in $K_{/\mathbb{Q}}$, every $A \in \mathcal{A}_{E,p}$ has finite $\underline{III}_K(A)[\mathfrak{p}_A^\infty]$ and $\mathrm{Sel}_K(A)[\mathfrak{p}_A^\infty]$ as long as $p \notin S_E$.*

§17. More concrete statement.

Corollary C. *Let* $N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$ *(all the cases when* $X_0(N)$ *is an elliptic curve with finite* $X_0(N)(\mathbb{Q})$*). Pick an admissible prime* p *for* $X_0(N)$*. Then* $|\underline{\underline{III}}_{\mathbb{Q}}(A)[\mathfrak{p}_A^\infty]| < \infty$ *and* $|\mathrm{Sel}_{\mathbb{Q}}(A)[\mathfrak{p}_A^\infty]| < \infty$ *for almost all* A *in* $\mathcal{A}_{X_0(N),p}$*. If further* $X_0(N)(\mathbb{Q})_p = \underline{\underline{III}}_{\mathbb{Q}}(X_0(N))_p = 0$, $\mathrm{Sel}_{\mathbb{Q}}(A)[\mathfrak{p}_A^\infty]$ *and* $\underline{\underline{III}}_{\mathbb{Q}}(A)[\mathfrak{p}_A^\infty]$ *are both finite for all* A *in* $\mathcal{A}_{X_0(N),p}$ *without exception.*

If E *is the factor of* $J_0(37)$ *with root number* -1 *(so,* $\mathrm{rank}\, E(\mathbb{Q}) = 1$*), for an admissible prime* p *for* E*, we have* $|\underline{\underline{III}}_{\mathbb{Q}}(A)[\mathfrak{p}_A^\infty]| < \infty$ *for almost all* A *in* $\mathcal{A}_{E,p}$*.*

§18. Conjecture.

Here is a conjecture:

Conjecture 1. *Let* Spec($\mathbb{I}$) *be a new irreducible component of* Spec($\mathbf{h}_{\alpha,\delta}$)*, and pick a totally real field* K*.*
(1) Suppose $(\alpha,\delta) = (1,1)$ *and that the root number of* $\mathbb{I}$ *is* $\epsilon := \pm 1$ *over the totally real number field* K*. Then for almost all* $P \in \Omega_{\mathbb{I}}$*, we have* $\dim_{H_P} A_P(K) \otimes_{\mathbb{Z}} \mathbb{Q} = \frac{1-\epsilon}{2}$*.*
(2) Suppose $(\alpha,\delta) \neq (1,1)$*. Then for almost all* $P \in \Omega_{\mathbb{I}}$*, we have* $\dim_{H_P} A_P(K) \otimes_{\mathbb{Z}} \mathbb{Q} = 0$*.*

Combined with the solution of the parity conjecture by Nekovar and Dokchitser/Dokchitser with our result, the above conjecture holds in many cases.

§19. Start of the proof for $\underline{\text{Ш}}(\mathcal{G}) := \underline{\text{Ш}}(\mathbb{Q}^S/\mathbb{Q}, \mathcal{G})$ for $K = \mathbb{Q}$.

Recall the 1st fundamental sequence: $0 \to A_P[p^\infty] \to \mathcal{G} \xrightarrow{\varpi} \mathcal{G} \to 0$. Then we get a commutative diagram with exact bottom two rows and exact columns:

$$\begin{array}{ccccccc}
\mathrm{Ker}(\iota_{\text{Ш},*}) & \longrightarrow & \underline{\text{Ш}}(A_P^{\mathrm{ord}}[p^\infty]) & \xrightarrow{\iota_{\text{Ш},*}} & \underline{\text{Ш}}(\mathcal{G}) & \xrightarrow{\varpi_{\text{Ш},*}} & \underline{\text{Ш}}(\mathcal{G}) \\
\cap\downarrow & & \cap\downarrow & & \cap\downarrow & & \cap\downarrow \\
E_{BT}^\infty(K) & \xrightarrow{\hookrightarrow} & H^1(A_P^{\mathrm{ord}}[p^\infty]) & \xrightarrow{\iota_*} & H^1(\mathcal{G}) & \xrightarrow{\varpi_*} & H^1(\mathcal{G}) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\prod_{v \in S} E_{BT}^\infty(K_v) & \xrightarrow{\hookrightarrow} & H_S^1(A_P^{\mathrm{ord}}[p^\infty]) & \xrightarrow{\iota_{S,*}} & H_S^1(\mathcal{G}) & \xrightarrow{\varpi_{S,*}} & H_S^1(\mathcal{G}),
\end{array}$$

where $E_{BT}^\infty(k) = \mathrm{Coker}(\varpi : \mathcal{G}(k) \to \mathcal{G}(k))$ and $H_S^1(?) = \prod_{l \in S} H^1(K_l, ?)$.

§20. Conclusion of the proof for $\underline{\text{III}}(\mathcal{G})$.

If $a_p \not\equiv 1 \mod p$, we have $\mathcal{G}(\mathbb{Q}) = \mathcal{G}(\mathbb{Q}_p) = 0$. If the residual representation of ρ_{f_P} is irreducible, again $\mathcal{G}(\mathbb{Q}) = 0$. It is easy to show $E^\infty_{BT}(K)$ and $\prod_{v \in S} E^\infty_{BT}(K_v)$ are finite. Thus the sequence

$$0 \to \underline{\text{III}}(A^{\text{ord}}_P[p^\infty]) \to \underline{\text{III}}(\mathcal{G}) \to \underline{\text{III}}(\mathcal{G})$$

is exact up to finite error. Thus if $\underline{\text{III}}(A^{\text{ord}}_{P_0}[p^\infty])$ is finite, the Pontryagin dual $\underline{\text{III}}(\mathcal{G})^\vee$ is a torsion $\mathbb{T}$-module of finite type; so, for most $P \in \Omega_{\mathbb{T}}$, $|\underline{\text{III}}(A^{\text{ord}}_P[p^\infty])| < \infty$. □

§21. Start of the proof for $\mathrm{Sel}(A_P^{\mathrm{ord}}) := \mathrm{Sel}_K(A_P^{\mathrm{ord}})$ for $K = \mathbb{Q}$.

Recall the following second fundamental exact sequence:

$$0 \to A_P^{\mathrm{ord}}(K') \to J_\infty^{\mathrm{ord}}(K') \xrightarrow{\varpi} J_\infty^{\mathrm{ord}}(K') \to B_P^{\mathrm{ord}}(K') \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to 0,$$

where $J_\infty^{\mathrm{ord}} = \varinjlim_s J_s^{\mathrm{ord}}$ and $K' = \mathbb{Q}^S$ and $\overline{\mathbb{Q}}_l$. We separate it into two short exact sequences:

$$0 \to A_P^{\mathrm{ord}}(K') \to J_\infty^{\mathrm{ord}}(K') \xrightarrow{\varpi} \varpi(J_\infty^{\mathrm{ord}})(K') \to 0,$$
$$0 \to \varpi(J_\infty^{\mathrm{ord}})(K') \to J_\infty^{\mathrm{ord}}(K') \to B_P^{\mathrm{ord}}(K') \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to 0.$$

§22. The proof for $\mathrm{Sel}(A_P^{\mathrm{ord}})$ continues.

Look into the following commutative diagram of sheaves with exact rows:

$$\begin{array}{ccccccc}
A_P[p^\infty]^{\mathrm{ord}} & \stackrel{\hookrightarrow}{\longrightarrow} & J_\infty^{\mathrm{ord}}[p^\infty] & \xrightarrow{\varpi[p^\infty]} & J_\infty^{\mathrm{ord}}[p^\infty] & \longrightarrow & 0 \\
\downarrow & & \downarrow & & i\downarrow & & \downarrow \\
A_P^{\mathrm{ord}} & \stackrel{\hookrightarrow}{\longrightarrow} & J_\infty^{\mathrm{ord}} & \xrightarrow{\varpi} & J_\infty^{\mathrm{ord}} & \longrightarrow & B_r^{\mathrm{ord}} \otimes \mathbb{Q}_p.
\end{array}$$

Since $B_r^{\mathrm{ord}} \otimes \mathbb{Q}_p$ is a sheaf of $\mathbb{Q}_p$-vector spaces and $J_\infty^{\mathrm{ord}}[p^\infty]$ is p-torsion, the inclusion map i factors through the image $\mathrm{Im}(\varpi) = \varpi(J_\infty^{\mathrm{ord}})$; so,

$$\varpi(J_\infty^{\mathrm{ord}})[p^\infty] = J_\infty^{\mathrm{ord}}[p^\infty].$$

§23. **Injectivity of** $\mathrm{Sel}(\varpi(J_\infty^{\mathrm{ord}})) \to \mathrm{Sel}(J_\infty^{\mathrm{ord}})$.

From the exact sequence, $\varpi(J^{\mathrm{ord}}) \hookrightarrow J^{\mathrm{ord}} \twoheadrightarrow B_r^{\mathrm{ord}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, taking its cohomology sequence, we get the bottom sequence of the following commutative diagram with exact rows:

$$\begin{array}{ccccc} 0 & \longrightarrow & H^1(\varpi(J_\infty^{\mathrm{ord}})[p^\infty]) & = & H^1(J_\infty^{\mathrm{ord}}[p^\infty]) \\ \downarrow & & \downarrow i & & \downarrow \\ \prod_{l \in S} E^*_{\mathrm{Sel}}(\mathbb{Q}_l) & \xrightarrow{\hookrightarrow} & H^1_S(\varpi(J_\infty^{\mathrm{ord}})) & \xrightarrow{\twoheadrightarrow} & H^1_S(J_\infty^{\mathrm{ord}}), \end{array}$$

where we have written $H^1_S(X) := \prod_{v \in S} H^1(K_v, X)$ and

$$E^*_{\mathrm{Sel}}(\mathbb{Q}_l) := \mathrm{Coker}(J_\infty^{\mathrm{ord}}(K_v) \to B_r^{\mathrm{ord}}(K_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p).$$

§24. Conclusion for injectivity.

By the snake lemma, we get an exact sequence

$$0 \to \mathsf{Sel}_K(\varpi(J_\infty^{\mathsf{ord}})) \to \mathsf{Sel}_K(J_\infty^{\mathsf{ord}}) \to \prod_{v|p} E^*_{\mathsf{Sel}}(K_v),$$

since it is easy to see $B_P^{\mathsf{ord}}(\mathbb{Q}_l) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = E^*_{\mathsf{Sel}}(\mathbb{Q}_l) = 0$ if $l \neq p$.

§25. Hard part.

We look into:

$$\begin{array}{ccccccc}
\mathrm{Ker}(\iota_*) & \xrightarrow{i_0} & \mathrm{Sel}(A_P^{\mathrm{ord}}) & \xrightarrow{\iota_*} & \mathrm{Sel}(J_{\infty,\mathbb{T}}^{\mathrm{ord}}) & \xrightarrow{\varpi_*} & \mathrm{Sel}(\varpi(J_{\infty,\mathbb{T}}^{\mathrm{ord}})) \\
i\downarrow & & \cap\downarrow a & & \cap\downarrow & & \cap\downarrow \\
E_{BT}(\mathbb{Q}) & \xrightarrow{\hookrightarrow} & H^1(A_P^{\mathrm{ord}}[p^\infty]) & \xrightarrow{\iota_*} & H^1(\mathcal{G}) & \xrightarrow{\varpi_*} & H^1(\mathcal{G}) \\
e\downarrow & & \downarrow & & \downarrow & & \downarrow \\
E^\infty(\mathbb{Q}_p) & \xrightarrow[e_0]{\hookrightarrow} & H^1_S(A_P^{\mathrm{ord}}) & \xrightarrow{\iota_{S,*}} & H^1_S(J_{\infty,\mathbb{T}}^{\mathrm{ord}}) & \xrightarrow[\twoheadrightarrow]{\varpi_*} & H^1_S(\varpi(J_{\infty,\mathbb{T}}^{\mathrm{ord}})).
\end{array}$$

Here $E^\infty(k) = \varinjlim_s \frac{\alpha(J_{\infty,\mathbb{T}}^{\mathrm{ord}})(k)}{\alpha(J_{\infty,\mathbb{T}}^{\mathrm{ord}}(k))}$. The error $E^\infty(\mathbb{Q}_p)$ injects into

$$H^1(\mathbb{Q}_p[\mu_{p^\infty}]/\mathbb{Q}_p, A_P^{\mathrm{ord}}(\mathbb{Q}_p[\mu_{p^\infty}])).$$

§26. Conclusion.

If A_P has good reduction modulo p, by a result of P. Schneider on universal norm, $|E^\infty(\mathbb{Q}_p)| \leq |H^1(\mathbb{Q}_p[\mu_{p^\infty}]/\mathbb{Q}_p, A_P^{\mathrm{ord}}(\mathbb{Q}_p[\mu_{p^\infty}])| = |A_P(\mathbb{F}_p)|^2$. If A_P has good reduction over $\mathbb{Z}_p[\mu_{p^r}]$, we have an exact sequence for $K_r = \mathbb{Q}_p[\mu_{p^r}]$:

$$\begin{aligned} &H^1(K_r/K, A_P^{\mathrm{ord}}(K_r)) \to H^1(K_\infty/K, A_P^{\mathrm{ord}}(K_\infty)) \\ &\quad \to H^0(K_r/K, H^1(K_\infty/K_r, A_P^{\mathrm{ord}}(K_\infty)) \to H^2(K_r/K, A_P^{\mathrm{ord}}(K_r)), \end{aligned}$$

we get the finiteness of $E^\infty(\mathbb{Q}_p)$.

As already seen, $E_{BT}(\mathbb{Q})$ is finite, we get an exact sequence

$$0 \to \mathrm{Sel}(A_P^{\mathrm{ord}}) \to \mathrm{Sel}(J_{\infty,\mathbb{T}}^{\mathrm{ord}}) \xrightarrow{\varpi} \mathrm{Sel}(J_{\infty,\mathbb{T}}^{\mathrm{ord}})$$

and hence if $\mathrm{Sel}(A_{P_0}^{\mathrm{ord}})$ is finite, $\mathrm{Sel}(J_{\infty,\mathbb{T}}^{\mathrm{ord}})^\vee$ is $\mathbb{T}$-torsion, so, $\mathrm{Sel}(A_P^{\mathrm{ord}})$ is finite for most of P.

§27. Case where $\mathrm{Sel}(A^{\mathrm{ord}}_{P_0}) = 0$.

If $\mathrm{Sel}(A^{\mathrm{ord}}_{P_0}) = 0$ and A_{P_0} has good reduction modulo p with $A^{\mathrm{ord}}_{P_0}(\mathbb{F}_p) = 0$, again by Schneider, the sequence

$$0 \to \mathrm{Sel}(A^{\mathrm{ord}}_{P_0}) \to \mathrm{Sel}(J^{\mathrm{ord}}_{\infty,\mathbb{T}}) \to \mathrm{Sel}(J^{\mathrm{ord}}_{\infty,\mathbb{T}})$$

is exact, and hence $\mathrm{Sel}(J^{\mathrm{ord}}_{\infty,\mathbb{T}}) = 0$. This shows that finiteness of $\mathrm{Sel}(A^{\mathrm{ord}}_P)$ for all $P \in \Omega_{\mathbb{T}}$.

§28. **Sketch for $\underline{\mathrm{III}}(A^{\mathrm{ord}})$.** Assume that $\underline{\mathrm{III}}_K(A_{P_0}[p^\infty]^{\mathrm{ord}})$ is finite (this follows from $\dim_{H_{P_0}} A^{\mathrm{ord}}_{P_0}(K) \otimes \mathbb{Q} \leq 1$ and $|\underline{\mathrm{III}}_K(A^{\mathrm{ord}}_{P_0})| < \infty$ by Kummer theory). Then from the sheaf exact sequence:

$$0 \to A^{\mathrm{ord}}_{P_0}[p^\infty] \to A^{\mathrm{ord}}_{P_0} \oplus \varpi(J^{\mathrm{ord}}_\infty) \xrightarrow{\pi} J^{\mathrm{ord}}_\infty \to 0,$$

by a diagram chasing, we get the finiteness of the kernel of

$$\underline{\mathrm{III}}_K(\varpi(J^{\mathrm{ord}}_{\infty,\mathbb{T}})) \to \underline{\mathrm{III}}_K(J^{\mathrm{ord}}_{\infty,\mathbb{T}}).$$

Then similarly to the control of the Selmer group, we get the following exact sequence up to finite error:

$$0 \to \underline{\mathrm{III}}_K(A^{\mathrm{ord}}_{P_0}) \to \underline{\mathrm{III}}_K(J^{\mathrm{ord}}_{\infty,\mathbb{T}}) \xrightarrow{\varpi} \underline{\mathrm{III}}_K(J^{\mathrm{ord}}_{\infty,\mathbb{T}}).$$

Then in the same way as Selmer group, we get $\mathbb{T}$-torsion property of $\underline{\mathrm{III}}_K(J_{\infty,\mathbb{T}})^{\mathrm{ord},\vee}$, and by some more argument finiteness of $\underline{\mathrm{III}}_K(A^{\mathrm{ord}}_P)$ with $\dim_{H_P} A_P(K) \otimes \mathbb{Q} \leq 1$ for most P.