* Non-abelian “class number” formula for the adjoint Selmer groups and cyclicity

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

A talk at AMS meeting in Hawaii, March, 2019.

*The author is partially supported by the NSF grant: DMS 1464106.

For a given elliptic cusp form f, we have a 2-dimensional p-adic Galois representation ρ with coefficients in a p-adic integer ring. Having ρ act on SL(2)-Lie algebra $\mathfrak{sl}_2$ by adjoint (conjugate action), we get a 3-dimensional representation Ad. We describe the formula of the order of the p-adic arithmetic cohomology group Sel(Ad) (called the adjoint Selmer group) via the L-value $L(1, Ad) = L(1, Ad(f))$ and explore the question when the Selmer group is cyclic (having one generator) over the coefficient ring? A detailed proof of the results described in this note is posted as a series of pdf slide files in my graduate course web page (`http://www.math.ucla.edu/~hida/207a.1.19w/index.html`). The section number given in the text is the section number of this graduate course.

§0. Set-up.

• Fix a prime $p \geq 5$; $\overline{\rho} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$: an **odd** representation unramified outside $0 < N \in \mathbb{Z}$ ($\mathbb{F}/\mathbb{F}_p$ finite) irreducible over $\mathbb{Q}[\mu_p]$; $W_{/\mathbb{Z}_p} \subset \overline{\mathbb{Q}}_p$: a discrete valuation ring with residue field $\mathbb{F}$.

• $F(\overline{\rho}) = \overline{\mathbb{Q}}^{\mathrm{Ker}(\overline{\rho})}$, $F^{(p)}(\overline{\rho})$: the maximal p-profinite extension of $F(\overline{\rho})$ **unramified outside** p, $\mathcal{G} := \mathrm{Gal}(F^{(p)}(\overline{\rho})/\mathbb{Q})$. Fix a decomposition subgroup $D_l \subset \mathcal{G}$ of l with its inertia subgroup I_l.

• Assume $\overline{\rho}|_{D_p} = \begin{pmatrix} \overline{\epsilon} & * \\ 0 & \overline{\delta} \end{pmatrix}$; $\overline{\delta} \neq \overline{\epsilon}$; $\overline{\delta}$ unramified.

• $(R, \boldsymbol{\rho} : \mathcal{G} \to \mathrm{GL}_2(R))$: the universal pair among p-ordinary deformations with coefficients in local p-profinite W-algebras with residue field $\mathbb{F}$. This means $\mathcal{F}(A) \cong \mathrm{Hom}_{W\text{-alg}}(R, A)$ for

$$\mathcal{D}(A) = \{\rho : \mathcal{G} \to \mathrm{GL}_2(A) | \rho \bmod \mathfrak{m}_A = \overline{\rho} \text{ with } \rho|_{D_p} = \left(\begin{smallmatrix} \epsilon & * \\ 0 & \delta \end{smallmatrix}\right)\},$$
$$\mathcal{F}(A) = \mathcal{D}(A)/(1 + M_2(\mathfrak{m}_A)) \cong \mathrm{Hom}_{CNL}(R, A) \text{ (unramified } \delta).$$

• Assume that the ramification index of $F(\overline{\rho})/\mathbb{Q}$ of any prime is prime to p (the minimally ramified case).

• Define $Ad(\rho)$ by the conjugation action via ρ on $\mathfrak{sl}_2(A) \subset \mathrm{End}_A(\rho)$.

§1. Serre's modulo p modularity conjecture.

Write $\det(\overline{\rho}) = \overline{\nu}_p^{k-1}\psi$ ($k \geq 1$) for the p-adic cyclotomic character $\overline{\nu}_p$ modulo p and a Dirichlet character ψ of conductor N.

Theorem 1 (Khare-Wintenberger). *There exists a Hecke eigenform $f \in S_k(\Gamma_0(N), \psi)$ ($k \geq 2$) with q-expansion coefficients in a valuation ring $W_{/\mathbb{Z}_p}$ such that ρ_f mod $\mathfrak{m}_W \cong \overline{\rho}$.*

When $k = 1$, we allow f in the theorem to be ordinary p-adic Hecek eigenform. There could be finitely many such f for a fixed k. Let $\mathbb{T}$ be the algebra generated over W by Hecke operators T acting on $\overline{\mathbb{Q}}_p$-span of all such f's $V := \sum_f \overline{\mathbb{Q}}_p f$. $\mathbb{T}$ is a local ring over W with $\mathbb{T}/\mathfrak{m}_{\mathbb{T}} = \mathbb{F}$. We have the modular representation $\rho_{\mathbb{T}} : \mathcal{G} \to \mathrm{GL}_2(\mathbb{T})$ such that $\mathrm{Tr}(\rho_{\mathbb{T}}(\mathrm{Frob}_l)) = T(l)|_V$. Write $f|T = \lambda(T)f$ with an algebra homomorphism $\lambda : \mathbb{T} \twoheadrightarrow W$, and decompose $\mathbb{T} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathrm{Frac}(W) \oplus (\mathfrak{a} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ for $\mathfrak{a} := \mathrm{Ker}(\lambda)$ (algebra direct sum). For the image S of $\mathbb{T}$ in $\mathfrak{a} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, define **congruence modules** by

$$\boxed{C_0 := S \otimes_{\mathbb{T},\lambda} W = S/\mathfrak{a} \text{ and } C_1 = \Omega^1_{\mathbb{T}/\mathbb{Z}_p} \otimes_{\mathbb{T},\lambda} W = \mathfrak{a}/\mathfrak{a}^2} \text{(§1.5–11).}$$

§2. Adjoint Selmer order formula (§4.18, 9.2, 9.4, 9.9).

By Wiles–Taylor, we have a W-algebra isomorphism $\boxed{R \cong \mathbb{T}}$ which brings $\boldsymbol{\rho}$ to $\rho_{\mathbb{T}}$. Pick $\rho \in \mathcal{D}(A)$, and define $\mathcal{G}$-module $Ad(\rho)^* := Ad(\rho) \otimes_A A^\vee$ ($\vee$: Pontryagin dual). Write $U_p \subset H^1(D_p, Ad(\rho))$ for the subspace spanned by classes of cocycles upper-triangular on D_p and upper-nilpotent on I_p. Put $U_l :=$ Ker$(H^1(D_l, Ad(\rho)^*) \to H^1(I_l, Ad(\rho)^*))$ if $l \neq p$. Define, for the inertia subgroup I_l,

$$\mathrm{Sel}(Ad(\rho)) := \mathrm{Ker}(H^1(\mathcal{G}, Ad(\rho)^*) \xrightarrow{\prod_l \mathrm{Res}} \prod_{l|Np} H^1(D_l, Ad(\rho)^*))/U_l.$$

Define the **dual Selmer group** Sel$^\perp(Ad(\rho)(1))$ replacing U_l by its orthogonal complement $U_l^\perp$ under local Tate duality. We have the following result for $\rho = \rho_f$ associated to a cusp form f:

$$|L(1, Ad(\rho))/*|_p^{-1} \overset{\text{Hida}}{=} |C_0| \overset{\text{Tate, Wiles}}{=} |C_1| \overset{\text{Mazur}}{=} |\mathrm{Sel}(Ad(\rho))|,$$

where "$*$" is a canonical period (the period determinant of f).

§3. Number of generators of R (§4.7, 4.9).

As is well known in deformation theory,

$$\boxed{t_R^* := \mathfrak{m}_R/\mathfrak{m}_R^2 + \mathfrak{m}_W = \Omega_{R/W} \otimes_R \mathbb{F} \cong \mathrm{Sel}(Ad(\overline{\rho}))^\vee}.$$

Here "$\vee$" denotes Pontryagin dual. So the number of generators of $R_{/W}$ is $r_0 := \dim_{\mathbb{F}} \mathrm{Sel}(Ad(\overline{\rho}))$. More generally, by Mazur

$$\boxed{\Omega_{R/W} \otimes_{R,\varphi} A \cong \mathrm{Sel}(Ad(\rho))^\vee} \text{ (Selmer control §4.18)}$$

for all $\rho \in \mathcal{D}(A)$ with $\varphi \circ \boldsymbol{\rho} \cong \rho$.

Recall the dual Selmer group

$$\mathrm{Sel}^\perp(Ad(\overline{\rho})(1)) := \mathrm{Ker}(H^1(\mathcal{G}, Ad(\overline{\rho})(1)) \to \prod_{l|Np} H^1(D_l, Ad(\overline{\rho}))/U_l^\perp)$$

An important fact (§5.7) due to Greenberg and Wiles is

Theorem 2. $r_0 = \dim_{\mathbb{F}} \mathrm{Sel}(Ad(\overline{\rho})) \leq \dim_{\mathbb{F}} \mathrm{Sel}^\perp(Ad(\overline{\rho})(1)) =: r$.

The right hand side is often **computable** by Kummer theory.

§4. Presentation Theorem: $\mathbb{T} \cong \frac{W[[X_1,\dots,X_r]]}{(S_1,\dots,S_r)}$ (§9.4).

To prove their "$R = \mathbb{T}$" theorem, Taylor and Wiles proved the existence of a presentation as above, where $r = \dim_{\mathbb{F}} \mathrm{Sel}^{\perp}(Ad(\overline{\rho})(1))$.

On the other hand, the minimal number of generators of $R = \mathbb{T}$ is given by the dimension r_0 of its co-tangent space $\mathbb{F}$-dual to $\mathrm{Sel}(Ad(\overline{\rho}))$. By a general ring theory (for example, Matsumura's book Theorem 21.2 (ii) in Cambridge study series), we can reduce the number of variables to $r_0 \le r$; so,

$$\mathbb{T} \cong \frac{W[[T_1,\dots,T_{r_0}]]}{(s_1,\dots,s_{r_0})} \quad \text{(local complete intersection over } W\text{)}.$$

This implies $|C_0| = |C_1|$ by Tate, and

$$\boxed{\mathrm{Sel}(Ad(\rho))^{\vee} \cong C_1 = \Omega_{\mathbb{T}/W} \otimes_{\mathbb{T},\varphi} A = \frac{A \cdot dT_1 + \cdots + A \cdot dT_{r_0}}{A \cdot ds_1 + \cdots + A \cdot ds_{r_0}}.}$$

§**5. Cyclicity: When $r = 1$?** Let $F := \overline{\mathbb{Q}}^{\ker(Ad(\overline{\rho}))}$ with integer ring O and $G :=$ Gal$(F/\mathbb{Q}) \cong$ Im$(Ad(\overline{\rho}))$. By Kummer theory, Sel$^{\perp}(Ad(\overline{\rho})(1))$ (restricted to the stabilizer $\mathcal{H}$ of F in $\mathcal{G}$) is generated by Kummer cocycle $u(\sigma) = \sqrt[p]{\alpha}^{(\sigma-1)}$ for $\alpha \in F^{\times}$ **very unramified**. Let $\widehat{O}^{\times} = O^{\times} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Assume $\boxed{\widehat{O}^{\times} = \mathbb{Z}_p[G]\varepsilon}$ (cyclicity of $\widehat{O}^{\times}$ over $\mathbb{Z}_p[G]$) for a Minkowski unit $\varepsilon \in O^{\times}$ which is implied by $\boxed{p \nmid |G|}$ (i.e., $\overline{\rho}$ is a reduction of an **Artin representation** ρ). Hard to know about Cl_F; so, we assume $\boxed{p \nmid |Cl_F[Ad]|}$ for Ad-isotypical component $Cl_F[Ad]$. Essentially by unramifiedness of u, **cyclicity** is implied by (§5.12)

$$\boxed{\dim_{\mathbb{F}} \mathrm{Sel}^{\perp}(Ad(\overline{\rho})(1)) \leq \dim_{\mathbb{F}} \mathrm{Hom}_{\mathbb{F}[G]}(O^{\times} \otimes \mathbb{F}, Ad(\overline{\rho})) =: r_1.}$$

Without $p \nmid |Cl_F[Ad]|$, if $r_1 \leq 1$, we get an exact sequence for $\rho = \rho_f$ for f classical of weight 1 (§7.10, 8.6),

$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(Cl_F, Ad(\rho)^*) \hookrightarrow \mathrm{Sel}(Ad(\rho)) \twoheadrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(\widehat{O}_{\mathfrak{p}}^{\times}[\delta^{-1}\epsilon]/\overline{\langle \varepsilon_{\delta^{-1}\epsilon} \rangle}, W^{\vee}),$$

where and $\varepsilon_{\epsilon\delta^{-1}}$ is the projection of ε in the $\epsilon\delta^{-1}$-eigenspace $\widehat{O}_{\mathfrak{p}}^{\times}[\epsilon\delta^{-1}] \subset \widehat{O}_{\mathfrak{p}}^{\times}$ for the prime $\mathfrak{p}|p$ associated to D_p.

§6. Proof of cyclicity by Dirichlet's unit theorem (§5.17):

Theorem 3. *Assume* $(O^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \mathbb{Z}_p[G]\varepsilon$ *or* $p \nmid |G|$. *Then we have* $\dim_{\mathbb{F}} \mathrm{Hom}_{\mathbb{F}[G]}(O^\times \otimes \mathbb{F}, Ad(\overline{\rho})) \leq \dim_{\mathbb{F}} Ad(\overline{\rho})^{c=1} = 1$.

By the proof of Dirichlet's unit theorem, for the subgroup C generated by a complex conjugation c,

$$(O^\times \otimes_{\mathbb{Z}} \mathbb{Q}) \oplus \mathbb{Q} \cong \mathbb{Q}[G/C] = \mathrm{Ind}_C^G \mathbb{Q} \quad \text{and hence}$$
$$\mathbb{Z}_p[G/C] \hookrightarrow (O^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p) \oplus \mathbb{Z}_p \hookrightarrow \mathbb{Z}_p[G/C] \cong \mathrm{Ind}_C^G \mathbb{Z}_p.$$

Assuming $(O^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p) = \mathbb{Z}_p[G]\varepsilon$, the above inclusions are isomorphisms, and by Shapiro's lemma,

$$\mathrm{Hom}_{\mathrm{Gal}(F/\mathbb{Q})}(O^\times \otimes_{\mathbb{Z}} \mathbb{F}, Ad(\overline{\rho})) \hookrightarrow \mathrm{Hom}_{\mathbb{F}[G]}(\mathrm{Ind}_C^G \mathbb{Z}_p, Ad(\overline{\rho}))$$
$$= \mathrm{Hom}_{\mathbb{F}[C]}(\mathbb{Z}_p, Ad(\overline{\rho})) \cong Ad(\overline{\rho})^{c=1} \text{ (the } c\text{-fixed subspace).}$$

Since $Ad(\overline{\rho})(c) \sim \mathrm{diag}[-1, 1, -1]$, we get $\dim_{\mathbb{F}} \mathrm{Sel}(Ad(\overline{\rho})(1)) \leq 1$.

§7. Qustions towards general cyclicity.

Starting the compatible system $\{\rho_{\mathfrak{p}}\}$ associated to a cusp form f, if $F := F(Ad(\overline{\rho}_{\mathfrak{p}}))$ for $\overline{\rho}_{\mathfrak{p}} = \rho_{\mathfrak{p}}$ mod $\mathfrak{p}$ is independent of p, $p \nmid |Cl_F|$ gives a condition for cyclicity; i.e., when $\overline{\rho}$ is a reduction modulo p of an Artin representation. Assuming $\overline{\rho}$ comes from an Artin representation, we proved cyclicity of Sel$(Ad(\rho_{\mathfrak{p}}))^{\vee}$ over W, which implies cyclicity of Sel$(Ad(\boldsymbol{\rho}))^{\vee}$ over $\mathbb{T}$ (even if Sel$(Ad(\rho_{\mathfrak{p}}))$, Sel$(Ad(\boldsymbol{\rho}))$ and $\mathbb{T}$ depend on $\mathfrak{p}$).

In the general non-Artin case, fundamental questions are:

Is $\mathfrak{p} \nmid |Cl_F[Ad]|$ for most $\mathfrak{p}$ (even if F depends on $\mathfrak{p}$)?

and only thing we need for cyclicity of Sel$(Ad(\rho))$ and Sel$(Ad(\boldsymbol{\rho}))$ is cyclicity of $O^{\times} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ over $\mathbb{Z}_p[G]$; so,

Is $O^{\times} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ cyclic as $\mathbb{Z}_p[G]$-modules for most of $\mathfrak{p}$?

For $\mathfrak{p}$ for which the above questions are affirmative, Sel$(Ad(\rho))^{\vee}$ is cyclic over A for every $\rho \in \mathcal{D}(A)$.