Iwasawa's dream

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

A talk at Hokkaido Univ., Sapporo, June 28, 2024, Japan.

We first discuss Conjectures/Problems (in cyclotomic theory) Iwasawa described in one of his final unpublished manuscripts [U3]. Then if time allows, we indicate which of his problems has generalizations in more general settings of adjoint Selmer groups via the theory of modular forms. In the general case, the Iwasawa algebra is replaced by a universal deformation ring (which is a p-adic Hecke algebra by a theorem of Taylor–Wiles). We encounter new interesting features related to Iwasawa's question in the general case. We fix a prime $p \geq 5$ throughout this lecture.

§1. Iwasawa's cyclotomic tower.

Iwasawa studied p-cyclotomic fields (in 1950s): the field $F_n = \mathbb{Q}(\mu_{p^n})$ generated by the group $\mu_{p^n}(\mathbb{C}) = \left\{\zeta_{p^n}^a := \exp(\frac{2\pi i a}{p^n})\right\}_{a=1}^{p^n}$ of p^n-th roots of unity, and put $F_\infty = \bigcup_n F_n \subset \mathbb{C}$. Its Galois group

$$G_n := \mathrm{Gal}(F_n/\mathbb{Q}) \xrightarrow[\nu_n]{\sim} (\mathbb{Z}/p^n\mathbb{Z})^\times,\ G_\infty := \mathrm{Gal}(F_\infty/\mathbb{Q}) \xrightarrow[\nu]{\sim} \mathbb{Z}_p^\times$$

with ν_n^{-1} sending $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ to the field automorphism σ_a taking $\zeta_{p^n} = \exp(\frac{2\pi i}{p^n})$ to $\zeta_{p^n}^a = \exp(\frac{2\pi i a}{p^n})$. Let $O_n := \mathbb{Z}[\mu_{p^N}]$. Though F_∞ depends on p, $\nu(\mathrm{Frob}_l) = l$ independent of p if $l \neq p$.

Let $\mathcal{H}_n$ be the maximal abelian unramified extension of F_n (Hilbert class field). Then $\mathrm{Gal}(\mathcal{H}_n/F_n)$ is canonically isomorphic to

$$Cl_n := \mathrm{Pic}(O_n) = \frac{\{\text{fractional ideals of } F_n\}}{\{(\alpha)|\alpha \in F_n^\times\}} \quad \text{(the class group)}$$

such that a prime $\mathfrak{l} \nmid p$ goes to $\mathrm{Frob}_\mathfrak{l}$ (Frobenius at $\mathfrak{l}$). Let C_n be maximal p-group quotient of Cl_n.

§**2. Minus part.** Put $Cl_n^- = Cl_n/Cl_n^{c+1}$ for complex conjugation c and $Cl_n^+ = \mathrm{Ker}(Cl_n \to Cl_n^-)$. Write H_n for the subfield of $\mathcal{H}_n$ such that $\mathrm{Gal}(H_n/F_n) \cong C_n^-$ (p-Hilbert class field).

We know a formula of the order of Cl_n^- due to Dirichlet (1839; Gauss 1801?) and Kummer:

Theorem: $|Cl_n^-| = 2p^n \prod_{\chi:(\mathbb{Z}/p^n\mathbb{Z})^\times \to \mathbb{C}^\times;\chi(-1)=-1} \frac{1}{2}L(0,\chi^{-1})$ with $L(0,\chi^{-1}) = -\frac{1}{p^n}\sum_{a=1}^{p^n} \chi^{-1}(a)a$.

Here $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_l (1-\chi(l)l^{-s})^{-1}$ (Dirichlet L).

The character χ extends to a algebra homomorphism χ of the group algebra $\mathbb{Z}[G_n]$ to $\mathbb{Z}[\chi]$. We then replace $\frac{1}{p^n}\sum_{a=1}^{p^n} \chi^{-1}(a)a$ by its preimage $\theta = \theta_n := \sum_{a=1}^{p^n} \frac{a}{p^n}\sigma_a^{-1} \in \mathbb{Q}[G_n]$ (Stickelberger's element); so, we have $\chi(\theta_n) = -L(0,\chi)$.

§**3. Stickelberger's theorem.** By $\chi(\theta_n) = -L(0,\chi)$, we imagine that θ would kill Cl_n^-. The group algebar $\mathbb{Z}[G_n]$ acts on Cl_n by $\mathfrak{a}^\xi = \prod_\sigma \mathfrak{a}^{\sigma a_\sigma}$ for $\xi := \sum_\sigma a_\sigma \sigma \in \mathbb{Z}[G_n]$. We put $\mathfrak{S}_n := (\theta_n) \cap \mathbb{Z}[G_n]$ which is called the Stickerberger ideal of F_n. By Kummer (1847) for F_1 and by Stickelberger (1890),

$$\boxed{\mathfrak{S}_n \text{ annihilates } Cl_n^-} \quad (\textbf{but often } \mathbb{Z}[G_n]/\mathfrak{S}_n \not\cong Cl_n^-).$$

The obstruction may be Cl_n^+ if non-trivial. We look at the p-primary part $C_n^\pm := Cl_n^\pm \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Kummer (and Vandiver) conjectured triviality of C_1^+:

KVC conjecture: $\boxed{C_1^+ = \{1\}}$ (no p-obstruction ?) which implies $C_n^+ = \{1\}$.

We do not have a convincing evidence except for numerical computation for primes up to more than two billion (up to 2,147,483,648, W. Hart, D. Harvey, W. Ong, 2017).

§**4. Iwasawa algebra.** For $m > n$ and $R_n = \mathbb{Z}_p[G_n]$:

- $R_m \xrightarrow{\mathrm{Res}_{m,n}} R_n$ given by $\sigma \mapsto \sigma|_{F_n}$ with $\theta_m \mapsto \theta_n$ and

$$\boxed{R_\infty := \mathbb{Z}_p[[\mathbb{Z}_p^\times]] = \varprojlim_n R_n \cong \mathbb{Z}_p[\zeta][[T]] \quad \text{for primitive } \zeta^{p-1} = 1,}$$

- $C_m^- \to C_n^-$ by the norm maps $\mathfrak{a} \mapsto \prod_{\sigma \in \mathrm{Ker}(\mathrm{Res}_{m,n})} \mathfrak{a}^\sigma$ and the R_∞-module $\boxed{C_\infty^- := \varprojlim_n C_n^- \cong \mathrm{Gal}(H_\infty/F_\infty)}$ $(H_\infty = \bigcup_n H_n)$.

Since $\mathbb{Z}_p[\zeta] \cong \prod_{j=1}^{p-1} \mathbb{Z}_p$ by the j-th projection $\omega_j(\zeta) = \zeta^j$, we have

$\boxed{R_\infty \cong \prod_{j=0}^{p-2} \Lambda}$ for $\Lambda = \mathbb{Z}_p[[T]]$ (one variable power series ring).

The R_∞-module C_∞^- is called an **Iwasawa module**, and Λ is called the **Iwasawa algebra**. Then the odd j-component $L_j(T) := \theta_\infty^{(j)}(T)$ is the p-adic L-function: $L_j((1+p)^s - 1)|_{s=1-k} = L(1-k, \omega_{j-k+1})$ for $0 < k \in \mathbb{Z}$ (Iwasawa 1969).

§5. Cyclicity, 1969

Iwasawa's theorem: *Let* $X_j := \omega_j C_\infty^-$ *for an odd* j*. Then as a module over* Λ*, under KVC,* $X_j \cong \Lambda/(L_j(T)) \Rightarrow C_n^- \cong R_n/\mathfrak{S}_n R_n$.

Cyclicity Conjecture: $X_j \cong \Lambda/(L_j(T))$ *up to finite error always.*

The zeros of the Riemann zeta function are expected to be all simple and lie in a special line: $\frac{1}{2} + \mathbb{R}\sqrt{-1}$?

Semi-simplicity Conjecture: *The zeros of* $L_j(T)$ *are simple and lie on* $\mathbb{Z}_p$*; so,* $L_j(T) = \prod_i (T - \alpha_i)U$ $(U \in \Lambda^\times)$ *with* $\alpha_i \neq \alpha_{i'}$ $(i \neq i')$.

The following version has been verified up to two billion.

Linearity Question/conjecture: *The number of zeros of* L_j *is less than or equal to* 1*; i.e.,* $L_j(T) = (T - \alpha)U$ *or* U *with* $U \in \Lambda^\times$.

Plainly

$$\text{Linearity} \Rightarrow \text{Semi-simplicity} \overset{\text{Chinese Remainder Thm}}{\Rightarrow} \boxed{\text{Cyclicity}}.$$

These Conjectures are open and made in [U3] in 1987.

§6. Cyclotomic theory to deformation theory.

Instead of roots of unity, take a rational elliptic curve which provides $r := \{r_p\}_p$ a system of 2-dim absolutely irreducible Galois representations into $\mathrm{GL}_2(\mathbb{Z}_p)$ with $\mathrm{Tr}(r_p(\mathrm{Frob}_l)), \det(r_p(\mathrm{Frob}_l)) \in \mathbb{Z}$ independent of $l \nmid Np$ for an integer $N > 0$. Take r_p with absolutely irreducible $\overline{\rho} = r_p \mod (p)$ with reducible $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \sim \begin{pmatrix} \epsilon & * \\ 0 & \delta \end{pmatrix}$ $(\overline{\epsilon} \neq \overline{\delta})$. Hereafter we vary a complete local $\mathbb{Z}_p$-algebra A with $A/\mathfrak{m}_A = \mathbb{F}_p$. A representation ρ of $\mathcal{G} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with values in $\mathrm{GL}_2(A)$ is a **p-ordinary** deformation of $\overline{\rho}$ if $\rho \mod \mathfrak{m}_A = \overline{\rho}$ and

(ord_p) $\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \sim \begin{pmatrix} \epsilon & * \\ 0 & \delta \end{pmatrix}$ *with δ unramified ($\delta \mod \mathfrak{m}_A = \overline{\delta}$), ρ unramified over $\overline{\mathbb{Q}}^{\mathrm{Ker}(\overline{\rho})}$ outside p.*

There exists a universal pair $(R, \boldsymbol{\rho})$ for a complete local $\mathbb{Z}_p$-algebra R with and a p-ordinary deformation $\boldsymbol{\rho} : \mathcal{G} \to \mathrm{GL}_n(R)$ **dependent** on p such that

$$\boxed{\mathrm{Hom}_{W\text{-alg}}(R, A) = \{\rho : \mathcal{G} \to \mathrm{GL}_2(A) : p\text{-ordinary} | (\rho \mod \mathfrak{m}_A) \sim \overline{\rho}\}/\cong}$$

by $\rho \leftrightarrow \varphi$ if $\rho \sim \varphi \circ \boldsymbol{\rho}$ for $\varphi \in \mathrm{Hom}_{CL_W}(R, A)$.

§7. Selmer groups for a 3-dimensional representation.

The group $X_j^\vee$ has an interpretation of the unramified subgroup of $H^1(\mathbb{Q}, \omega_j(R_\infty)^\vee)$ ("$\vee$" denotes Pontryagin dual). Let $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ act on $\mathfrak{sl}_2(A)$ by $x \mapsto \rho(\sigma)x\rho(\sigma)^{-1}$ and write rank 3 representation as $\boxed{Ad(\rho)}$. So we get a compatible system $Ad(r) = \{Ad(r_p)\}$, and a well defined subgroup $\mathrm{Sel}(Ad(\rho))$ of $H^1(\mathbb{Q}, Ad(\rho) \otimes A^\vee)$. We replace (Λ, X_j) by $(R, \mathrm{Sel}(Ad(\boldsymbol{\rho}))^\vee)$.

$\mathrm{Sel}(Ad(\boldsymbol{\rho}))^\vee$ is cyclic $\Leftrightarrow$ R is generated at most one element over Λ.

By myself and Taylor–Wiles, R is **free and finite** over Λ, and $\mathrm{Spec}(R)$ has densely populated points of modular Galois deformations r'_p for modular r' of weight $k > 2$. There is a p-adic L-function $L_p : \mathrm{Spec}(R) \ni \rho \mapsto L_p(\rho) \in \mathbb{C}_p$ ($L_p \in R$) interpolating $L(1, Ad(r'))/\Omega_{r'}$. Here is the Selmer class number formula:

If $\overline{\rho}$ is irreducible over $\mathbb{Q}[\zeta_p]$,

$$|\mathrm{Sel}(Ad(r_p))| = |L_p(r_p)|_p^{-1} \quad \textit{and} \quad |L_p(r'_p)|_p = \left|\frac{L(1, Ad(r'))}{\Omega_{r'}}\right|_p.$$

§8. Cyclicity theorem:

If $\overline{\rho}$ is absolutely irreducible over $\mathbb{Q}[\zeta_p]$, $\mathrm{Sel}(Ad(\rho))^\vee \cong A/(L_p(\rho))$ for primes p outside an explicit finite set E of p-ordinary primes dependent on r.

In place of an elliptic curve, we may start with a modular form of weight k. Under $k > 2$, if $E := \{p|\frac{L(1,Ad(r))}{\Omega_r} = L_p(r_p)\}$, $\mathrm{Sel}(Ad(\rho)) = 0$ for $p \notin E$. If $k = 2$, $E := \{p|\frac{L(1,Ad(r))}{\Omega_r}\}$. For infinitely many (level raising) primes p, $\frac{L(1,Ad(r))}{\Omega_r} \neq L_p(r_p)$, and $\mathrm{Sel}(Ad(\boldsymbol{\rho}))$ is infinite but cyclic if $p \notin E$. If $k = 1$, r is an Artin representation independent of p (by Deligne–Serre). If r is induced from a real quadratic field F, $\mathrm{Sel}(Ad(\boldsymbol{\rho}))$ is infinite for all ordinary p splitting in F but is cyclic for all p prime to class number h of $\overline{\mathbb{Q}}^{\mathrm{Ker}(Ad(r))}$ ($E = \{p|h\}$). For the cases $k \neq 2$, see my book published in 2022 from World Scientific.

If $p \nmid L_p(r_p)$, then $R \cong \Lambda$, and hence R is regular.

§**9. Wall-Sun-Sun primes.** Assume $k = 1$. Then for primes with positive density, r_p is p-ordinary. As we remarked in §7, if R is a regular local ring, then $\mathrm{Sel}(Ad(\boldsymbol{\rho}))^\vee$ is cyclic.

A question asked by C. Khare and G. Böckle is

Question. *What is the distribution of primes p with regular R assuming r_p is p-ordinary?*

Suppose $r = \mathrm{Ind}_F^{\mathbb{Q}} \varphi$ for a real quadratic field F. If p splits into $\mathfrak{p}\mathfrak{p}'$ in F prime to the class number h_F, regularity of R is equivalent to $\varepsilon^{p-1} \not\equiv 1 \mod \mathfrak{p}^2$ for the fundamental unit ε of F. Primes with $\varepsilon^{p-1} \equiv 1 \mod \mathfrak{p}^2$ (Wall-Sun-Sun primes) are conjectured to be infinitely many (but perhaps zero density) by analytic number theorists (no example up to 9.7×10^{17} when $F = \mathbb{Q}[\sqrt{5}]$, but some for $F \neq \mathbb{Q}[\sqrt{5}]$).