ON A GENERALIZATION OF THE CONJECTURE OF MAZUR–TATE–TEITELBAUM

HARUZO HIDA

Abstract. We propose a generalization of the conjecture of Mazur-Tate-Teitelbaum (predicting an exact shape of the p-adic $\mathcal{L}$-invariant of rational Tate curves (which is now a theorem of Greenberg-Stevens) to the symmetric powers of motivic two dimensional odd Galois representations over totally real fields. At p-adic places where the motive is multiplicative, the $\mathcal{L}$-invariant is conjectured to have the same shape as predicted by them. Then we prove our conjecture assuming a precise ring theoretic structure of the universal infinitesimal Galois deformation ring of the symmetric power.

1. The conjectures

Let p be an odd prime and F be a totally real field of degree $d < \infty$ with integer ring O. Order the prime factors of p in O as $\mathfrak{p}_1, \dots, \mathfrak{p}_g$. In this talk, we describe the computation of Greenberg's $\mathcal{L}$-invariant $\mathcal{L}_{n,m}$ (at $s = m$) of the symmetric n-th powers ρ_n of the Tate module T_pE for an elliptic curve $E_{/F}$ with multiplicative reduction at $\mathfrak{p}_j|p > 2$ for $j = 1, 2, \dots, b$ and ordinary good reduction at $\mathfrak{p}_j|p$ for $j > b$. Greenberg and also myself in different ways proved under some assumptions, for the number e of vanishing modifying Euler p-factors at m for m critical for ρ_n, the characteristic power series $L_p(s, \rho_n)$ of $\mathrm{Sel}_{F_\infty}(\rho_n \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ for the cyclotomic $\mathbb{Z}_p$-extension F_∞/F vanishes of order $\geq e$ at $s = m$:

$$\lim_{s\to m} \frac{L_p(s, \rho_n)}{(s-m)^e} \sim \mathcal{L}(\rho_{n,m}) \big|\#(\mathrm{Sel}_F(\rho_n \otimes \mathbb{Q}_p/\mathbb{Z}_p))\big|_p^{-1},$$

where $\sim$ means up to units.

Write F_i for $F_{\mathfrak{p}_i}$, $E(\overline{F}_i) = \overline{F}_i^\times/q_i^{\mathbb{Z}}$ for $i \leq b$, $Q_i = N_{F_i/\mathbb{Q}_p}(q_i)$, and $\Gamma_i = \mathcal{N}(\mathrm{Gal}(\overline{F}_i/F_i)) \cap (1 + p\mathbb{Z}_p)$ for the p-adic cyclotomic character $\mathcal{N}$. We assume throughout the talk that *E does not have complex multiplication.* Take an algebraic closure $\overline{F}$ of F. Writing $\rho_0 : \mathrm{Gal}(\overline{F}/F) \to GL_2(\mathbb{Q}_p)$ for the Galois representation on T_pE, put $\rho_n = \rho_{n,0} = Sym^{\otimes n}(\rho_0)$ and $\rho_{n,m} = \rho_n(-m) = \rho_n \otimes \det(\rho_0)^{-m}$. Note that $\rho_E|_{D_\mathfrak{p}} \sim \left(\begin{smallmatrix} \beta_\mathfrak{p} & * \\ 0 & \alpha_\mathfrak{p} \end{smallmatrix}\right)$ ($D_\mathfrak{p} = \mathrm{Gal}(\overline{F}_\mathfrak{p}/F_\mathfrak{p})$) with unramified $\alpha_\mathfrak{p}$ at each prime factor $\mathfrak{p}|p$. Let $S_{n,m}$ be the set of prime ideals of O where $\rho_{n,m}$ ramifies. Consider $J_1 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. We then define $J_n = Sym^{\otimes n}(J_1)$. Define an algebraic group G_n over $\mathbb{Z}_p$ by

$$G_n(R) = \left\{\xi \in GL_{n+1}(R) \middle| {}^t\xi J_n \xi = \nu(\xi) J_n\right\} \quad (\text{for } \mathbb{Z}_p\text{-algebras } R)$$

Date: July 2, 2008.

A conference talk at Irsee (Germany) on 6/30/08. The author is partially supported by the NSF grant: DMS 0244401, DMS 0456252 and DMS 0753991.

with the similitude homomorphism $\nu : G_n \to \mathbb{G}_m$. Then G_n is a quasi-split orthogonal or symplectic group according as n is even or odd. The representation $\rho_{n,0}$ of $\mathrm{Gal}(\overline{F}/F)$ factors through $G_n(K) \subset GL_{n+1}(K)$.

Let $K/\mathbb{Q}_p$ be a finite extension with p-adic integer ring W. Start with $\rho_{n,0}$ and consider the deformation ring $(R_n, \boldsymbol{\rho}_n)$ which is universal among the following deformations: Galois representations $\rho_A : \mathrm{Gal}(\overline{F}/F) \to G_n(A)$ for Artinian local K-algebras A with residue field $K = A/\mathfrak{m}_A$ (for the maximal ideal $\mathfrak{m}_A$ of A) such that

(K$_n$1) unramified outside $S_{n,0}$, ∞ and p;

(K$_n$2) for all prime factors $\mathfrak{p}$ of p, $\rho_A|_{D_\mathfrak{p}} \cong \begin{pmatrix} \alpha_{0,A,\mathfrak{p}} & * & \cdots & * \\ 0 & \alpha_{1,A,\mathfrak{p}} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{n,A,\mathfrak{p}} \end{pmatrix}$ with $\alpha_{j,A,\mathfrak{p}} \equiv \beta_\mathfrak{p}^{n-j}\alpha_\mathfrak{p}^j$ mod $\mathfrak{m}_A$ and $\alpha_{j,A,\mathfrak{p}}|_{I_\mathfrak{p}}$ $(j = 0, 1, \ldots, n)$ factoring through $\mathrm{Gal}(F_\mathfrak{p}[\mu_{p^\infty}]/F_\mathfrak{p})$;

(K$_n$3) $\nu \circ \rho_A = \nu \circ \rho_{n,0} = \det(\rho_0)^n$ in A;

(K$_n$4) $\rho_A \equiv \rho_{n,0} \mod \mathfrak{m}_A$.

Since $\rho_{n,0}$ is absolutely irreducible and all $\alpha_\mathfrak{p}^i\beta_\mathfrak{p}^{n-i}$ for $i = 0, 1, \ldots, n$ are distinct, the deformation problem specified by (K$_n$1–4) is representable by a universal couple $(R_n, \boldsymbol{\rho}_n)$. In other words, for any ρ_A as above, there exists a unique K-algebra homomorphism $\varphi : R_n \to A$ such that $\varphi \circ \boldsymbol{\rho}_n \approx \rho_A$. Here $\rho \approx \rho'$ if and only if $\rho' = x\rho x^{-1}$ for $x \in G_n(A)$ whose image in $G_n(A/\mathfrak{m}_A)$ is trivial. The representation ρ is said to be *strictly* equivalent to ρ' if $\rho \approx \rho'$. Often we fix $n > 0$ and write simply $(R, \boldsymbol{\rho})$ for $(R_n, \boldsymbol{\rho}_n)$.

Write now

$$\boldsymbol{\rho}_n|_{D_\mathfrak{p}} \cong \begin{pmatrix} \boldsymbol{\delta}_{0,\mathfrak{p}} & * & \cdots & * \\ 0 & \boldsymbol{\delta}_{1,\mathfrak{p}} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \boldsymbol{\delta}_{n,\mathfrak{p}} \end{pmatrix}$$

with $\boldsymbol{\delta}_{j,\mathfrak{p}} \equiv \beta_\mathfrak{p}^{n-j}\alpha_\mathfrak{p}^j \mod \mathfrak{m}_n$ (for $\mathfrak{m}_n = \mathfrak{m}_{R_n}$). Let $\Gamma_\mathfrak{p}$ be the maximal torsion-free quotient of the inertia group of $\mathrm{Gal}(F_\mathfrak{p}[\mu_{p^\infty}]/F_\mathfrak{p})$. Then the character $\widehat{\boldsymbol{\delta}}_{j,\mathfrak{p}} := \boldsymbol{\delta}_{j,\mathfrak{p}}(\beta_\mathfrak{p}^{n-j}\alpha_\mathfrak{p}^j)^{-1}$ restricted to the $\mathfrak{p}$-inertia subgroup $I_\mathfrak{p}$ factors through $\Gamma_\mathfrak{p}$, giving rise to an algebra structure of R_n over $W[[\Gamma_\mathfrak{p}]]$. Take the product $\boldsymbol{\Gamma} = \prod_{\mathfrak{p}|p} \Gamma_\mathfrak{p}^{n+1}$ of $n+1$ copies of $\Gamma_\mathfrak{p}$ over all prime factors $\mathfrak{p}$ of p in F. We write general elements of $\boldsymbol{\Gamma}$ as $x = (x_{j,\mathfrak{p}})_{j,\mathfrak{p}}$ with $x_{j,\mathfrak{p}}$ in the j-th component $\Gamma_\mathfrak{p}$ in $\boldsymbol{\Gamma}$ $(j = 0, 1, \ldots, n)$. Consider the character $\widehat{\boldsymbol{\delta}} : \boldsymbol{\Gamma} \to R_n^\times$ given by $\widehat{\boldsymbol{\delta}}(x) = \prod_{j=0}^n \prod_{\mathfrak{p}|p} \widehat{\boldsymbol{\delta}}_{j,\mathfrak{p}}(x_{j,\mathfrak{p}})$. Choosing a generator $\gamma_i = \gamma_\mathfrak{p}$ (for $\mathfrak{p} = \mathfrak{p}_i$) of the topologically cyclic group $\Gamma_\mathfrak{p}$, we identify $W[[\boldsymbol{\Gamma}]]$ with a power series ring $W[[X_{j,\mathfrak{p}}]]_{j,\mathfrak{p}}$ by associating the generator $\gamma_j := \gamma_{\mathfrak{p}_j}$ of the j-th component $\Gamma_{\mathfrak{p}_j}$ of $\boldsymbol{\Gamma}$ with $1 + X_{j,\mathfrak{p}}$. The character $\widehat{\boldsymbol{\delta}} : \boldsymbol{\Gamma} \to R_n^\times$ extends uniquely to an algebra homomorphism $\widehat{\boldsymbol{\delta}} : W[[X_{j,\mathfrak{p}}]]_{j,\mathfrak{p}} \to R_n$ by the universality of the (continuous) group ring $W[[\boldsymbol{\Gamma}]]$. Thus R_n is naturally an algebra over $K[[X_{j,\mathfrak{p}}]]_{j,\mathfrak{p}}$.

Conjecture 1.1. *Suppose that n is odd. Then R_n is isomorphic to the power series ring $K[[X_{j,\mathfrak{p}}]]_{\mathfrak{p}|p, 1 \le j \le n,\ j:odd}$ of E variables for $E = g\frac{n+1}{2}$.*

Remark 1.2. (1) *If $n = 1$ and $F = \mathbb{Q}$, this conjecture: $R_1 = K[[X_1]]$ follows from Serre's mod p modularity conjecture (proven by Khare/Wintenberger/Kisin). Let*

$\overline{\rho}_0 = (\rho_0 \mod \mathfrak{m}_W)$. *By Taylor's potential modularity of* ρ_0 *with additional assumptions that* $\mathrm{Im}(\overline{\rho}_0)$ *is nonsoluble, we can prove this conjecture for* $n = 1$ *(via modularity theorems of Fujiwara, Kisin and Chen).*

(2) *One can conjecture the same assertion starting with a more general* $\rho_0 : \mathrm{Gal}(\overline{F}/F) \to GL_2(W)$ *satisfying*
   (a) *its image contains an open subgroup of* $SL_2(\mathbb{Z}_p)$*;*
   (b) *it is a member of a strictly compatible system;*
   (c) *its restriction to* $D_\mathfrak{p}$ *is equivalent to* $\left(\begin{smallmatrix}\beta_\mathfrak{p} & * \\ 0 & \alpha_\mathfrak{p}\end{smallmatrix}\right)$*;*
   (d) $\alpha_\mathfrak{p}$ *and* $\beta_\mathfrak{p}$ *factors through* $\Gamma_\mathfrak{p}$*;*
   (e) *up to finite order characters,* $\alpha_\mathfrak{p} = \mathcal{N}^{k_\mathfrak{p}}$ *and* $\beta_\mathfrak{p} = \mathcal{N}^{k'_\mathfrak{p}}$ *with* $k_\mathfrak{p} > k'_\mathfrak{p}$ *for each* $\mathfrak{p}|p$*, where* $\mathcal{N}$ *is the p-adic cyclotomic character.*

(3) *Note that* $G_3 \cong GSp(4)$ *is the spin cover of* $G_4 = GO(2,3)$*. Some progress has been made by A. Genestier and J. Tilouine towards the "*$R = T$*" theorem for* $GSp(4)$*-Hecke algebras (for* $F = \mathbb{Q}$*), there is a good prospect to get a proof of Conjecture 1.1 when* $n = 3$ *and 4. Further, when* $F = \mathbb{Q}$*, in view of the recent results of Clozel–Harris–Taylor and Taylor (in the paper proving the Sato–Tate conjecture for Tate curves), one would be able to treat general* n *in future not so far away.*

We propose the following generalization of a conjecture of Mazur–Tate–Teitelbaum:

Conjecture 1.3. *Recall* $Q_i = N_{F_i/\mathbb{Q}_p}(q_i)$*. Suppose criticality at* 1 *of the symmetric power motive* $Sym^{\otimes n}(M) \otimes \det(M)^{-m}$ *for the motive* $M := H_1(E)$ *with Tate twist by an integer* m*. Then if* $\rho_{n,m}$ *has an exceptional zero at* $s = 1$*, we have*

$$\mathcal{L}(\rho_{n,m}) = \begin{cases} \left(\prod_{i=1}^{b} \frac{\log_p(Q_i)}{\mathrm{ord}_p(Q_i)}\right)\mathcal{L}(m) & \text{for } \mathcal{L}(m) \in K^\times \text{ if } n = 2m \text{ with odd } m \ (e = g), \\ \prod_{i=1}^{b} \frac{\log_p(Q_i)}{\mathrm{ord}_p(Q_i)} & \text{if } n \neq 2m \ (e = b). \end{cases}$$

We have $\mathcal{L}(m) = 1$ *if* $b = g$*, and the value* $\mathcal{L}(1)$ *when* $b < g$ *is given by*

$$\mathcal{L}(1) = \det\left(\frac{\partial \boldsymbol{\delta}_{1,\mathfrak{p}_i}([p,F_i])}{\partial X_{1,\mathfrak{p}_j}}\right)_{i>b,j>b}\Big|_{X=0} \prod_{i>b} \frac{\log_p(\gamma_i)}{[F_i : \mathbb{Q}_p]\alpha_i([p,F_i])}$$

for the local Artin symbol $[p, F_i]$*, where we regard* γ_i *as an element of* $\mathbb{Z}_p^\times$ *where we regard* γ_i *as an element of* $\mathbb{Z}_p^\times$ *by the cyclotomic character* $\mathcal{N}$ *to have* $\log_p(\gamma_i) \in \mathbb{Q}_p$*.*

Again, we could have started with a more general ρ_0 and could have made a similar conjecture.

Theorem 1.4. Conjecture 1.1 *implies* Conjecture 1.3 *for Greenberg's* $\mathcal{L}$*-invariant.*

2. Sketch of Proof

Let S_n be the derived group of G_n, and consider the Lie algebra $\mathfrak{s}_n$ of S_n. Then $\sigma \in \mathrm{Gal}(\overline{F}/F)$ acts on $\mathfrak{s}_n$ by $X \mapsto \rho_n(\sigma)X\rho_n(\sigma)^{-1}$. Write this Galois module as $Ad(\rho_n)$. Then

$$Ad(\rho_n) \cong \bigoplus_{j:\text{odd},\ 1\leq j\leq n} \rho_{2j,j}. \tag{2.1}$$

Let us write $\mathfrak{m}_n$ for the maximal ideal of R_n. Then in the standard manner, we get the following identity of the (modified) Selmer group of Greenberg:

Lemma 2.1. *Suppose* Conjecture 1.1. *Then canonically*

$$\mathrm{Sel}_F^{cyc}(Ad(\rho_n)) \cong \mathrm{Hom}_{\mathbb{Q}_p}(\mathfrak{m}_n/\mathfrak{m}_n^2, \mathbb{Q}_p) = \bigoplus_{j:odd, 1\le j\le n} \bigoplus_{\mathfrak{p}|p} \mathbb{Q}_p \cdot dX_{j,\mathfrak{p}} \cong \bigoplus_{j:odd,1\le j\le n} \mathrm{Sel}_F^{cyc}(\rho_{2j,j}),$$

and we have $\dim_K \mathrm{Sel}_F^{cyc}(\rho_{2j,j}) = g = |\{\mathfrak{p}|p\}|$ *and* $\mathrm{Sel}_F(\rho_{2j,j}) = 0$ *for odd* j *with* $1 \le j \le n$.

The tangent space of $\mathrm{Spf}(R_n)$ is given by $\mathrm{Sel}_F^{cyc}(Ad(\rho_n))$ by a general nonsense. The Selmer cocycles are given by $c_{j,\mathfrak{p}} = \left(\left.\frac{\partial\rho_n}{\partial X_{j,\mathfrak{p}}}\right|_{X=0}\right)\rho_n^{-1}$. Here Greenberg's Selmer group over an extension M/F is given in the following way: We have a p-adic Hodge filtration on $\rho_{n,m}$ such that on $\mathcal{F}_\mathfrak{p}^i/\mathcal{F}_\mathfrak{p}^{i+1}$, $D_\mathfrak{p}$ act by $\mathcal{N}^i$. Let $\mathcal{F}_\mathfrak{p}^+ = \mathcal{F}_\mathfrak{p}^1$ and $\mathcal{F}_\mathfrak{p}^- = \mathcal{F}_\mathfrak{p}^0$. We put

$$L_\mathfrak{p} = \mathrm{Ker}(\mathrm{Res}: H^1(M_\mathfrak{p}, \rho_{n,m}) \to H^1(I_\mathfrak{p}, \frac{\rho_{n,m}}{\mathcal{F}_\mathfrak{p}^+})),$$

and for primes $\mathfrak{q}$ outside p

$$L_\mathfrak{q} = \mathrm{Ker}(\mathrm{Res}: H^1(M_\mathfrak{q}, \rho_{n,m}) \to H^1(I_\mathfrak{q}, \rho_{n,m})).$$

Then

$$\mathrm{Sel}_M(\rho_{n,m}) = \mathrm{Ker}(H^1(M, \rho_{n,m}) \to \prod_{\mathfrak{l}:\text{all primes}} \frac{H^1(M_\mathfrak{l}, \rho_{n,m})}{L_\mathfrak{l}}). \tag{2.2}$$

We define the "locally cyclotomic" Selmer group $\mathrm{Sel}_M^{cyc}(\rho_{n,m})$ replacing $L_\mathfrak{p}$ by

$$L_\mathfrak{p}^{cyc}(V) = \mathrm{Ker}(\mathrm{Res}: H^1(M_\mathfrak{p}, \rho_{n,m}) \to H^1(I_{\mathfrak{p},\infty}, \frac{\rho_{n,m}}{\mathcal{F}_\mathfrak{p}^+})),$$

where $I_{\mathfrak{p},\infty}$ is the inertia group of $\mathrm{Gal}(\overline{M}_\mathfrak{p}/M_\mathfrak{p}[\mu_{p^\infty}])$.

Take a basis of cocycles $\{c_\mathfrak{p}\}_{\mathfrak{p}|p}$ representing $\mathrm{Sel}_F^{cyc}(\rho_{2m,m})$ over K (indexed by $\{\mathfrak{p}|p\}$). Write $a_\mathfrak{p} : D_{\mathfrak{p}'} \to K$ for $c_\mathfrak{p} \mod \mathcal{F}_{\mathfrak{p}'}^+\rho_{2m,m}$ regarded as a homomorphism (identifying $\mathcal{F}_\mathfrak{p}^-\rho_{2m,m}/\mathcal{F}_\mathfrak{p}^+\rho_{2m,m}$ with the trivial $D_\mathfrak{p}$-module K). We now have two $e\times e$ matrices with coefficients in K: $A_m = \left(a_{\mathfrak{p}_i}([p, F_{\mathfrak{p}_j}])\right)_{i,j}$ and $B_m = \left(\log_p(\gamma_{\mathfrak{p}_i})^{-1}a_{\mathfrak{p}_i}([\gamma_{\mathfrak{p}_j}, F_{\mathfrak{p}_j}])\right)_{i,j}$. We can see fairly easily that Conjecture 1.1 for $\rho_{n,0}$ with all odd $1 \le n \le m$ implies that B_m is invertible. Then Greenberg's $\mathcal{L}$-invariant is defined by

$$\mathcal{L}(\rho_{2m,m}) = \mathcal{L}(\mathrm{Ind}_F^\mathbb{Q}\rho_{2m,m}) = \det(A_m B_m^{-1}). \tag{2.3}$$

The determinant $\det(A_m B_m^{-1})$ is independent of the choice of the basis $\{c_\mathfrak{p}\}_\mathfrak{p}$. We also have the relation $\boldsymbol{\delta}_{i,\mathfrak{p}}\boldsymbol{\delta}_{n-i,\mathfrak{p}} = \mathcal{N}^n$ for $i = 0, 1, \ldots, n$. Then $\{dX_{j,\mathfrak{p}} \leftrightarrow c_{j,\mathfrak{p}}\}_{j:odd,\mathfrak{p}|p}$ is a basis of $\bigoplus_{j:odd,0<j\le n}\mathrm{Sel}_F^{cyc}(\rho_{2j,j})$. Using the explicit form of $c_{j,\mathfrak{p}}$ projected down to $\rho_{2m,m}$ for odd $0 < m \le n$, we can compute the $\mathcal{L}$-invariant in the form described in the theorem. See the following paper for details:

[H07] H. Hida, On a generalization of the conjecture of Mazur–Tate–Teitelbaum, International Mathematics Research Notices, Vol. 2007, Article ID rnm102, 49 pages. doi:10.1093/imrn/rnm102

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