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 \( L \)-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 \( L \)-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 \( p \) as \( p_1, \ldots, p_j \). In this talk, we describe the computation of Greenberg’s \( L \)-invariant \( \mathcal{L}_{n,m} \) (at \( s = m \)) of the symmetric \( n \)-th powers \( \rho_n \) of the Tate module \( T_pE \) for an elliptic curve \( E/F \) with multiplicative reduction at \( p_j|p > 2 \) for \( j = 1, 2, \ldots, b \) and ordinary good reduction at \( p_j|p > j > b \). 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 \( \rho_n \), the characteristic power series \( L_p(s, \rho_n) \) of \( \text{Sel}_{F,\infty}(\rho_n \otimes \mathbb{Q}_p / \mathbb{Z}_p) \) for the cyclotomic \( \mathbb{Z}_p \)-extension \( F_\infty/F \) vanishes of order \( \geq e \) at \( s = m \):

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

where \( \sim \) means up to unites.

Write \( F_i \) for \( F_{p_i} \), \( E(F_i) = F_i^{\times} / q_i^\mathbb{Z} \) for \( i \leq b \), \( Q_i = \text{N}_{F_i / \mathbb{Q}_p}(q_i) \), and \( \Gamma_i = \mathcal{N}(\text{Gal}(F_i/F_i)) \cap (1 + p\mathbb{Z}_p) \) 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 \( \rho_0 : \text{Gal}(\overline{F}/F) \to GL_2(\mathbb{Q}_p) \) for the Galois representation on \( T_pE \), put \( \rho_n = \rho_{n,0} = \text{Sym}^{\otimes n}(\rho_0) \) and \( \rho_{n,m} = \rho_n(-m) = \rho_n \otimes \text{det}(\rho_0)^{-m} \). Note that \( \rho_{E/D_p} \sim \begin{pmatrix} \beta_p & * \\ 0 & \alpha_p \end{pmatrix} \) \( (D_p = \text{Gal}(\overline{F}_p / F_p)) \) with unramified \( \alpha_p \) at each prime factor \( p \)|\( p \). Let \( S_{n,m} \) be the set of prime ideals of \( O \) where \( \rho_{n,m} \) ramifies. Consider \( J_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \). We then define \( J_n = \text{Sym}^{\otimes n}(J_1) \). Define an algebraic group \( G_n \) over \( \mathbb{Z}_p \) by

\[
G_n(R) = \{ \xi \in GL_{n+1}(R) | ^t \xi J_n \xi = v(\xi) J_n \} \quad (\text{for } \mathbb{Z}_p\text{-algebras } R)
\]

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 $\text{Gal}(\overline{F}/F)$ 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 $(R_n, \rho_n)$ which is universal among the following deformations: Galois representations $\rho_A : \text{Gal}(\overline{F}/F) \to G_n(A)$ for Artinian local $K$-algebras $A$ with residue field $K = A/m_A$ (for the maximal ideal $m_A$ of $A$) such that

(Kn1) unramified outside $S_{n,0}$, $\infty$ and $p$;

(Kn2) for all prime factors $p$ of $p$, $\rho_A|_{D_p} \cong \begin{pmatrix} \alpha_{0,A,p} & * & \cdots & * \\ 0 & \alpha_{1,A,p} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{n,A,p} \end{pmatrix}$ with $\alpha_{j,A,p} \equiv \beta_p^{n-j} \alpha_p^j$ mod $m_A$ and $\alpha_{j,A,p}|_{D_p}$ ($j = 0, 1, \ldots, n$) factoring through $\text{Gal}(F_p[\mu_p^\infty]/F_p)$;

(Kn3) $\nu \circ \rho_A = \nu \circ \rho_{n,0} = \det(\rho_0)^n$ in $A$;

(Kn4) $\rho_A \equiv \rho_{n,0}$ mod $m_A$.

Since $\rho_{n,0}$ is absolutely irreducible and all $\alpha_p^i, \beta_p^{n-i}$ for $i = 0, 1, \ldots, n$ are distinct, the deformation problem specified by (Kn1–4) is representable by a universal couple $(R_n, \rho_n)$. In other words, for any $\rho_A$ as above, there exists a unique $K$-algebra homomorphism $\varphi : R_n \to A$ such that $\varphi \circ \rho_n \approx \rho_A$. Here $\rho \approx \rho'$ if and only if $\rho' = \rho x^p - 1$ for $x \in G_n(A)$ whose image in $G_n(A/m_A)$ is trivial. The representation $\rho$ is said to be strictly equivalent to $\rho'$ if $\rho \approx \rho'$. Often we fix $n > 0$ and write simply $(R, \rho)$ for $(R_n, \rho_n)$.

Write now

$$\rho_n|_{D_p} \cong \begin{pmatrix} \delta_{0,p} & * & \cdots & * \\ 0 & \delta_{1,p} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \delta_{n,p} \end{pmatrix}$$

with $\delta_{j,p} \equiv \beta_p^{n-j} \alpha_p^j$ mod $m_n$ (for $m_n = m_{R_n}$). Let $\Gamma_p$ be the maximal torsion-free quotient of the inertia group of $Gal(F_p[\mu_p^\infty]/F_p)$. Then the character $\hat{\delta}_{j,p} := \delta_{j,p}(\beta_p^{n-j} \alpha_p^j)^{-1}$ restricted to the $p$-inertia subgroup $I_p$ factors through $\Gamma_p$, giving rise to an algebra structure of $R_n$ over $W[[\Gamma_p]]$. Take the product $\Gamma = \prod_{p \mid \mathfrak{n}} \Gamma_p$ of $n + 1$ copies of $\Gamma_p$ over all prime factors $p$ of $p$ in $F$. We write general elements of $\Gamma$ as $x = (x_{j,p})_{j,p}$ with $x_{j,p}$ in the $j$-th component $\Gamma_p$ in $\Gamma$ ($j = 0, 1, \ldots, n$). Consider the character $\hat{\delta} : \Gamma \to R_n^\times$ given by $\hat{\delta}(x) = \prod_{j=0}^n \prod_{p \mid \mathfrak{n}_{j,p}} \hat{\delta}_{j,p}(x_{j,p})$. Choosing a generator $\gamma_i = \gamma_p$ (for $p = p_i$) of the topologically cyclic group $\Gamma_p$, we identify $W[[\Gamma]]$ with a power series ring $W[[X_{j,p}]]_{j,p}$ by associating the generator $\gamma_j := \gamma_{p_j}$ of the $j$-th component $\Gamma_{p_j}$ of $\Gamma$ with $1 + X_{j,p}$. The character $\hat{\delta} : \Gamma \to R_n^\times$ extends uniquely to an algebra homomorphism $\hat{\delta} : W[[X_{j,p}]]_{j,p} \to R_n$ by the universality of the (continuous) group ring $W[[\Gamma]]$. Thus $R_n$ is naturally an algebra over $K[[X_{j,p}]]_{j,p}$.

**Conjecture 1.1.** Suppose that $n$ is odd. Then $R_n$ is isomorphic to the power series ring $K[[X_{j,p}]]_{1 \leq j \leq n, j \text{ odd}}$ of $E$ variables for $E = g_{n+1}^2$.

**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
\( \overline{\rho}_0 = (\rho_0 \mod m_{W}) \). By Taylor's potential modularity of \( \rho_0 \) 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 \( \rho_0 : \text{Gal}(F/F) \to \text{GL}_2(W) \) satisfying

(a) its image contains an open subgroup of \( \text{SL}_2(\mathbb{Z}_p) \);
(b) it is a member of a strictly compatible system;
(c) its restriction to \( D_p \) is equivalent to \( \begin{pmatrix} \beta_p & 0 \\ \alpha_p & 1 \end{pmatrix} \);
(d) \( \alpha_p \) and \( \beta_p \) factors through \( \Gamma_p \);
(e) up to finite order characters, \( \alpha_p = N'^{k_p} \) and \( \beta_p = N'^{k'_p} \) with \( k_p > k'_p \) for each \( p \mid I_p \), where \( N' \) is the \( p \)-adic cyclotomic character.

(3) Note that \( G_3 \cong \text{GSp}(4) \) is the spin cover of \( G_4 = \text{GO}(2, 3) \). Some progress has been made by A. Genestier and J. Tilouine towards the "R = T" theorem for \( \text{GSp}(4) \)-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 \( Q_i = \mathbb{N}_{F_i/\mathbb{Q}_p}(q_i) \). Suppose criticality at 1 of the symmetric power motive \( \text{Sym}^{\otimes n}(M) \otimes \det(M)^{-m} \) 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

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

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

\[
\mathcal{L}(1) = \det \left( \frac{\partial \delta_{1,p,([p, F_i])}}{\partial X_{1,p_j}} \right)_{i>b, j>b} \bigg|_{X=0} \prod_{i>b} \frac{\log_p(\gamma_i)}{[F_i : \mathbb{Q}_p] \alpha_i([p, F_i])}
\]

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

Again, we could have started with a more general \( \rho_0 \) 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 \( \sigma \in \text{Gal}(\overline{F}/F) \) acts on \( \mathfrak{s}_n \) by \( X \mapsto \rho_n(\sigma)X\rho_n(\sigma)^{-1} \). Write this Galois module as \( \text{Ad}(\rho_n) \). Then

\[
\text{Ad}(\rho_n) \cong \bigoplus_{j \text{ odd}, 1 \leq j \leq n} \rho_{2j,j}.
\]
Let us write $m_n$ 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

$$\text{Sel}^{\text{qc}}_F(\text{Ad}(\rho_n)) \cong \text{Hom}_{\mathbb{Q}_p}(m_n/m_n^2, \mathbb{Q}_p) = \bigoplus_{j: \text{odd}, 1 \leq j \leq n} \bigoplus_{p \mid p} \mathbb{Q}_p \cdot dX_{j,p} \cong \bigoplus_{j: \text{odd}, 1 \leq j \leq n} \text{Sel}^{\text{qc}}_F(\rho_{2j,j}),$$

and we have $\dim_K \text{Sel}^{\text{qc}}_F(\rho_{2j,j}) = g = |\{p|p\}|$ and $\text{Sel}_F(\rho_{2j,j}) = 0$ for odd $j$ with $1 \leq j \leq n$.

The tangent space of $\text{Spf}(R_n)$ is given by $\text{Sel}^{\text{qc}}_F(\text{Ad}(\rho_n))$ by a general nonsense. The Selmer cocycles are given by $c_{j,p} = \left( \frac{\partial \rho_n}{\partial X_{j,p}} \bigg|_{X=0} \right) \rho_n^{-1}$. 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 $\mathcal{F}_p^{i}/\mathcal{F}_p^{i+1}$, $D_p$ act by $\mathcal{N}^i$. Let $\mathcal{F}_p^{+} = \mathcal{F}_p^{1}$ and $\mathcal{F}_p^{-} = \mathcal{F}_p^{0}$. We put

$$L_p = \text{Ker}(\text{Res} : H^1(M_p, \rho_{n,m}) \to H^1(I_p, \frac{\rho_{n,m}}{\mathcal{F}_p^+})), $$

and for primes $q$ outside $p$

$$L_q = \text{Ker}(\text{Res} : H^1(M_q, \rho_{n,m}) \to H^1(I_q, \rho_{n,m})).$$

Then

$$\text{Sel}_M(\rho_{n,m}) = \text{Ker}(H^1(M, \rho_{n,m}) \to \prod_{\text{all primes } l} \frac{H^1(M_l, \rho_{n,m})}{L_l}).$$

We define the “locally cyclotomic” Selmer group $\text{Sel}^{\text{qc}}_M(\rho_{n,m})$ replacing $L_p$ by

$$L_p^{\text{qc}}(V) = \text{Ker}(\text{Res} : H^1(M_p, \rho_{n,m}) \to H^1(I_p, \frac{\rho_{n,m}}{\mathcal{F}_p^+})), $$

where $I_{p,\infty}$ is the inertia group of $\text{Gal}(\overline{M_p}/M_p[p^{\infty}])$.

Take a basis of cocycles $\{c_p\}_{p|p}$ representing $\text{Sel}^{\text{qc}}_F(\rho_{2m,m})$ over $K$ (indexed by $\{p|p\}$). Write $a_p : D_p \to K$ for $c_p \mod \mathcal{F}_p^{+} \rho_{2m,m}$ regarded as a homomorphism (identifying $\mathcal{F}_p^{-} \rho_{2m,m}/\mathcal{F}_p^{+} \rho_{2m,m}$ with the trivial $D_p$-module $K$). We now have two $e \times e$ matrices with coefficients in $K$: $A_m = (a_p([p, F_p]))_{i,j}$ and $B_m = (\log_p(\gamma_p)^{-1} a_p([\gamma_p, F_p]))_{i,j}$. We can see fairly easily that Conjecture 1.1 for $\rho_{n,0}$ with all odd $1 \leq n \leq m$ implies that $B_m$ is invertible. Then Greenberg’s $\mathcal{L}$-invariant is defined by

$$\mathcal{L}(\rho_{2m,m}) = \mathcal{L}(\text{Ind}^Q_F \rho_{2m,m}) = \text{det}(A_m B_m^{-1}).$$

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


DEPARTMENT OF MATHEMATICS, UCLA, LOS ANGELES, CA 90095-1555, U.S.A.