An Elementary Proof of the Mazur-Tate-Teitelbaum Conjecture for Elliptic Curves

Dedicated to Professor John Coates on the occasion of his sixtieth birthday

Shinichi Kobayashi[1]

Received: November 29, 2005
Revised: February 15, 2006

Abstract. We give an elementary proof of the Mazur-Tate-Teitelbaum conjecture for elliptic curves by using Kato's element.

2000 Mathematics Subject Classification: 11F85, 11G05, 11G07, 11G40, 11S40.
Keywords and Phrases: elliptic curves, p-adic L-functions, Iwasawa theory, the Mazur-Tate-Teitelbaum conjecture, exceptional zeros, Kato's element.

1. Introduction

The p-adic L-function $L_p(E,s)$ of an elliptic curve E defined over $\mathbb{Q}$ has an extra zero at $s=1$ coming from the interpolation factor at p if E has split multiplicative reduction at the prime p. The Mazur-Tate-Teitelbaum conjecture (now a theorem of Greenberg-Stevens) describes the first derivative of $L_p(E,s)$ as

$$\frac{d}{ds}L_p(E,s)\,|_{s=1} = \frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\,\frac{L(E,1)}{\Omega_E^+}$$

where q_E is the Tate period of E coming from the p-adic uniformization of E at p, $\log_p$ is the Iwasawa p-adic logarithm, Ω_E^+ is the real period of E and $L(E,1)$ is the special value of the complex Hasse-Weil L-function at $s=1$.

Known proofs of this conjecture are classified into two kinds. One is, as Greenberg-Stevens [GS] did first, a proof using a global theory like Hida's universal ordinary deformation. The other is, as Kato-Kurihara-Tsuji [KKT] or Colmez [C] did, a proof based on local theory (except using Kato's element). Each kind of proof has its own importance but the latter type of proof makes it clear that the substantial facts behind this conjecture are of local nature. The p-adic L-function is the image of Kato's element via a purely local morphism,

[1]Supported by JSPS Postdoctoral Fellowships for Research Abroad.

the so called Coleman map or Perrin-Riou map. The extra zero phenomena discovered by Mazur-Tate-Teitelbaum is, in fact, a property of the local Coleman map.
In this paper, we prove a derivative formula (Theorem 4.1) of the Coleman map for elliptic curves by purely local and elementary method and we apply this formula to Kato's element to show the conjecture of Mazur-Tate-Teitelbaum. Of course, our proof is just a special and the simplest case of that in Kato-Kurihara-Tsuji [KKT] or Colmez [C] (they proved the formula not only for elliptic curves but for higher weight modular forms) but I believe that it is still worthwhile to write it down for the following reason. First, the important paper Kato-Kurihara-Tsuji [KKT] has not yet been published. Second, since we restrict ourselves to the case of elliptic curves, the proof is much simpler and elementary (of course, such a simple proof would be also known to specialists. In fact, Masato Kurihara informed me that Kato, Kurihara and Tsuji have two simple proofs and one is similar to ours). I hope that this paper would help those who are interested in the understanding of this interesting problem.

ACKNOWLEDGEMENT: I would like to wish Professor John Coates a happy sixtieth birthday, and to thank him for his contribution to mathematics, especially to Iwasawa theory. It is my great pleasure to dedicate this article to him on this occasion.
This paper was written during the author's visit at the university of Paris 6. He would like to thank P. Colmez and L. Merel for the accommodation. He also would like to thank K. Bannai and N. Otsubo for discussion. Finally, he is grateful to the referee for his careful reading of the manuscript.

2. A structure of the group of local units in $k_\infty/\mathbb{Q}_p$.

Let k_∞ be the (local) cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$ in $\mathbb{Q}_p(\zeta_{p^\infty}) := \cup_{n=0}^{\infty}\mathbb{Q}_p(\zeta_{p^n})$ with Galois group Γ and let k_n be its n-th layer in k_∞ with Galois group Γ_n. We identify the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$ with $\mathbb{Z}_p^\times$ by the cyclotomic character κ. Then Γ is identified with $1+p\mathbb{Z}_p$ and the torsion subgroup Δ of $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$ is regarded as $\mu_{p-1} \subset \mathbb{Z}_p^\times$.
Let U_n^1 be the subgroup of $\mathcal{O}_{k_n}^\times$ consisting of the elements which are congruent to 1 modulo the maximal ideal $\mathfrak{m}_n$ of $\mathcal{O}_{k_n}$.
Following the Appendix of Rubin [R] or [Ko], for a fixed generator $(\zeta_{p^n})_{n\in\mathbb{N}}$ of $\mathbb{Z}_p(1)$, we construct a certain canonical system of local points $(d_n)_n \in \varprojlim_n U_n^1$ and we determine the Galois module structure of U_n^1 by using these points. The idea of the construction of such a system is as follows. First we consider a certain formal group $\mathcal{F}$ isomorphic to $\widehat{\mathbb{G}}_m$ whose formal logarithm has a certain compatible property with the trace operator of k_∞. Then the system of local points is essentially the image of cyclotomic units by the isomorphism $\mathcal{F} \cong \widehat{\mathbb{G}}_m$.
We let

$$\ell(X) = \log(1+X) + \sum_{k=0}^{\infty}\sum_{\delta\in\Delta}\frac{(X+1)^{p^k\delta}-1}{p^k}.$$

This power series is convergent in $\mathbb{Q}_p[[X]]$ due to the summation $\sum_{\delta\in\Delta}$. It is straightforward to see that

$$\ell'(X) \in 1 + X\mathbb{Z}_p[[X]], \quad \ell(0) = 0, \quad (\varphi - p)\circ \ell(X) \in p\mathbb{Z}_p[[X]]$$

where φ is the Frobenius operator such that $(\varphi \circ \ell)(X) = \ell((X+1)^p - 1)$. Hence by Honda's theory, there is a formal group $\mathcal{F}$ over $\mathbb{Z}_p$ whose logarithm is given by ℓ, and $\iota(X) = \exp\circ\,\ell\,(X) - 1 \in \mathbb{Z}_p[[X]]$ gives an isomorphism of formal groups $\mathcal{F} \cong \widehat{\mathbb{G}}_m$ over $\mathbb{Z}_p$. (See for example, Section 8 of [Ko].) Take an element ε of $p\mathbb{Z}_p$ such that $\ell(\varepsilon) = p$ and we define

$$c_n := \iota((\zeta_{p^{n+1}} - 1)\,[+]_{\mathcal{F}}\,\varepsilon).$$

Since this element is fixed by the group Δ, this is an element of $\widehat{\mathbb{G}}_m(\mathfrak{m}_n)$. Then by construction, $d_n = 1 + c_n \in U_n^1$ satisfies the relation

$$\log_p(d_n) = \ell(\varepsilon) + \ell(\zeta_{p^{n+1}} - 1) = p + \sum_{k=0}^{n} \sum_{\delta\in\Delta} \frac{{\zeta_{p^{n+1-k}}}^{\delta} - 1}{p^k}.$$

Proposition 2.1. *i)* $(d_n)_n$ *is a norm compatible system and* $d_0 = 1$.
ii) Let u *be a generator of* U_0^1. *Then as* $\mathbb{Z}_p[\Gamma_n]$*-module,* d_n *and* u *generate* U_n^1*, and* d_n *generates* $(U_n^1)^{\mathrm{N}=1}$ *where* N *is the absolute norm from* k_n *to* $\mathbb{Q}_p$.

Proof. Since $\zeta_p - 1$ is not contained in $\mathfrak{m}_n$, the group $\widehat{\mathbb{G}}_m(\mathfrak{m}_n)$ does not contain p-power torsion points. Therefore to see i), it suffices to show the trace compatibility of $(\log_p(d_n))_n$, and this is done by direct calculations. For ii), we show that $(\iota^{-1}(c_n)^\sigma)_{\sigma\in\Gamma_n}$ and ε generate $\mathcal{F}(\mathfrak{m}_n)$ as $\mathbb{Z}_p$-module by induction for n. The proof is the same as that of Proposition 8.11 of [Ko] but we rewrite it for the ease of the reader. The case $n = 0$ is clear. For arbitrary n, we show that $\ell(\mathfrak{m}_n) \subset \mathfrak{m}_n + k_{n-1}$ and

$$\mathcal{F}(\mathfrak{m}_n)/\mathcal{F}(\mathfrak{m}_{n-1}) \cong \ell(\mathfrak{m}_n)/\ell(\mathfrak{m}_{n-1}) \cong \mathfrak{m}_n/\mathfrak{m}_{n-1}.$$

Here the first isomorphism is induced by the logarithm ℓ and the last isomorphism is by $(\mathfrak{m}_n + k_{n-1})/k_{n-1} \cong \mathfrak{m}_n/\mathfrak{m}_{n-1}$. As a set, $\mathcal{F}(\mathfrak{m}_n)$ is the maximal ideal $\mathfrak{m}_n$, and we write $x \in \mathcal{F}(\mathfrak{m}_n)$ in the form $x = \sum_{\delta\in\Delta}\sum_i a_i\,\zeta_{p^{n+1}}^{i\delta}$, $a_i \in \mathbb{Z}_p$. Then for $y = \sum_{\delta\in\Delta}\sum_i a_i\,\zeta_{p^n}^{i\delta} \in \mathfrak{m}_{n-1}$, we have that $x^p \equiv y \mod p\mathcal{O}_{k_n}$. Therefore for $k \geq 1$, we have

$$\sum_{\delta\in\Delta} \frac{(x+1)^{p^k\delta} - 1}{p^k} \equiv \sum_{\delta\in\Delta} \frac{(x^p+1)^{p^{k-1}\delta} - 1}{p^k} \equiv \sum_{\delta\in\Delta} \frac{(y+1)^{p^{k-1}\delta} - 1}{p^k} \mod \mathfrak{m}_n.$$

Hence we have $\sum_\delta \frac{(x+1)^{p^k\delta}-1}{p^k} \in \mathfrak{m}_n + k_{n-1}$. Since $\ell(x)$ is convergent, for sufficiently large k_0, we have $\sum_{k=k_0}^{\infty}\sum_\delta \frac{(x+1)^{p^k\delta}-1}{p^k} \in \mathfrak{m}_n$, and therefore $\ell(x)$ is contained in $\mathfrak{m}_n + k_{n-1}$. Since ℓ is injective on $\mathcal{F}(\mathfrak{m}_n)$ (there is no torsion point in $\mathcal{F}(\mathfrak{m}_n) \cong \widehat{\mathbb{G}}_m(\mathfrak{m}_n)$) and is compatible with the Galois action, we have $\ell\,(\mathfrak{m}_n) \cap k_{n-1} = \ell\,(\mathfrak{m}_{n-1})$. Therefore we have an injection

$$\ell(\mathfrak{m}_n)/\ell(\mathfrak{m}_{n-1}) \hookrightarrow (\mathfrak{m}_n + k_{n-1})/k_{n-1} \cong \mathfrak{m}_n/\mathfrak{m}_{n-1}.$$

By direct calculations, we have $\ell(\iota^{-1}(c_n)) \equiv \sum_\delta(\zeta^\delta_{p^{n+1}} - 1) \mod k_{n-1}$. Since $\sum_\delta(\zeta^\delta_{p^{n+1}} - 1)$ generates $\mathfrak{m}_n/\mathfrak{m}_{n-1}$ as a $\mathbb{Z}_p[\Gamma_n]$-module with respect to the usual addition, the above injection is in fact a bijection. Thus $(\iota^{-1}(c_n)^\sigma)_{\sigma\in\Gamma_n}$ generate $\mathcal{F}(\mathfrak{m}_n)/\mathcal{F}(\mathfrak{m}_{n-1})$. By induction $(\iota^{-1}(c_n)^\sigma)_{\sigma\in\Gamma_n}$ and ε generate $\mathcal{F}(\mathfrak{m}_n)$. Since $\widehat{\mathbb{G}}_m$ is isomorphic to $\mathcal{F}$ by ι, we have ii). □

Since $Nd_n = d_0 = 1$, by Hilbert's theorem 90, there exists an element $x_n \in k_n$ such that $d_n = x_n^\gamma/x_n$ for a fixed generator γ of Γ. We put $\pi_n = \prod_{\delta\in\Delta}(\zeta^\delta_{p^{n+1}} - 1)$. Then π_n is a norm compatible uniformizer of k_n. By the previous proposition, x_n can be taken of the form $x_n = \pi_n^{e_n} u_n$ for some integer e_n and $u_n \in (U_n^1)^{\mathrm{N}=1}$.

Proposition 2.2. *In the same notation as the above, we have*

$$p \equiv e_n\,(p-1)\log_p \kappa(\gamma) \mod p^{n+1}.$$

Proof. If we put

$$G(X) = \exp(p)\cdot \exp\circ\,\ell\,(X) = \exp\circ\,\ell\,(X[+]\varepsilon) \in 1 + (p, X)\mathbb{Z}_p[[X]],$$

then by definition

$$G_\sigma(\zeta_{p^{m+1}} - 1) = d_m^\sigma$$

where $G_\sigma(X) = G((X+1)^{\kappa(\sigma)} - 1)$ for $\sigma \in \Gamma$. By Proposition 2.1 ii), u_n is written as a product in the form $u_n = \prod (d_n^\sigma)^a$. If we put $H(X) = \prod G_\sigma(X)^a$, then $H(X)$ satisfies $H(\zeta_{p^{m+1}} - 1) = N_{k_n/k_m} u_n$ for $0 \le m \le n$. We put

$$F(X) = \left(\prod_{\delta\in\Delta} \frac{(X+1)^{\delta\kappa(\gamma)} - 1}{(X+1)^\delta - 1}\right)^{e_n} \frac{H((X+1)^{\kappa(\gamma)} - 1)}{H(X)}.$$

Then we have

$$G(X) \equiv F(X) \qquad \mod \frac{(X+1)^{p^{n+1}} - 1}{X}$$

since they are equal if we substitute $X = \zeta_{p^{m+1}} - 1$ for $0 \le m \le n$. Substituting $X = 0$ in this congruence and taking the p-adic logarithm, we have that $p \equiv e_n(p-1)\log_p \kappa(\gamma) \mod p^{n+1}$. □

3. The Coleman map for the Tate curve.

We construct the Coleman map for the Tate curve following the Appendix of [R] or Section 8 of [Ko]. See also [Ku]. In this section we assume that E is the Tate curve

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

where $q = q_E \in \mathbb{Q}_p^\times$ satisfying $|q|_p < 1$ and

$$s_k(q) = \sum_{n\ge1} \frac{n^k q^n}{1-q^n}, \quad a_4(q) = -s_3(q), \quad a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}.$$

Then we have the uniformization

$$\phi :\ {\mathbb{C}_p}^\times/q^{\mathbb{Z}} \cong E_q(\mathbb{C}_p), \qquad u \mapsto (X(u,q), Y(u,q))$$

where

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q),$$

$$Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q).$$

(Of course, we put $\phi(q^{\mathbb{Z}}) = O$.) This isomorphism induces the isomorphism of the formal groups $\widehat{\phi} : \widehat{\mathbb{G}}_m \cong \widehat{E}$. It is straightforward to see that the pull back by $\widehat{\phi}$ of the invariant differential $\omega_E = \frac{dx}{2y+x}$ on $\widehat{E}$ with the parameter $t = -x/y$ is the invariant differential $\omega_{\widehat{\mathbb{G}}_m} = \frac{dX}{1+X}$ on $\widehat{\mathbb{G}}_m$ with the parameter $X = u-1$. Hence $\widehat{\phi}$ is given by the power series $t = \exp_{\widehat{E}} \circ \log(1+X) - 1 \in \mathbb{Z}_p[[X]]$.
From now we identify $\widehat{\mathbb{G}}_m$ with $\widehat{E}$ by $\widehat{\phi}$. In particular, we regard $c_n \in \widehat{\mathbb{G}}_m(\mathfrak{m}_n)$ in the previous section as an element of $\widehat{E}(\mathfrak{m}_n)$.
Let $T = T_pE$ be the p-adic Tate module of E and $V = T \otimes \mathbb{Q}_p$. The cup product induces a non-degenerate pairing of Galois cohomology groups

$$(\ ,\ )_{E,n} :\ H^1(k_n, T) \times H^1(k_n, T^*(1)) \to H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p.$$

If there is no fear of confusion, we write $(\ ,\ )_{E,n}$ simply as $(\ ,\ )_E$. By the Kummer map, we regard $\widehat{E}(\mathfrak{m}_n)$ as a subgroup of $H^1(k_n, T)$. Then we define a morphism $\mathrm{Col}_n : H^1(k_n, T^*(1)) \to \mathbb{Z}_p[\Gamma_n]$ by

$$z \quad \longmapsto \sum_{\sigma\in\Gamma_n} (c_n^\sigma,\ z)_{E,n}\, \sigma.$$

This morphism is compatible with the natural Galois action and since the sequence $(c_n)_n$ is norm compatible, Col_n is also compatible for n with respect to the corestrictions and the natural projections. We define the Coleman map

$$\mathrm{Col} : \quad \varprojlim_n H^1(k_n, T^*(1)) \ \longrightarrow\ \Lambda = \mathbb{Z}_p[[\Gamma]]$$

as the projective limit of Col_n over all n.
We recall the dual exponential map. For every n let $\tan(E/k_n)$ denote the tangent space of E/k_n at the origin, and consider the Lie group exponential map

$$\exp_{E,n} :\ \tan(E/k_n) \to E(k_n) \otimes \mathbb{Q}_p.$$

The cotangent space $\mathrm{cotan}(E/k_n)$ is generated by the invariant differential ω_E over k_n, and we let ω_E^* be the corresponding dual basis of $\tan(E/k_n)$. Then there is a dual exponential map

$$\exp_{E,n}^* :\ H^1(k_n, V^*(1)) \longrightarrow \mathrm{cotan}(E/k_n) = k_n\, \omega_E,$$

which has a property

$$(x, z)_{E,n} = \mathrm{Tr}_{k_n/\mathbb{Q}_p} \log_{\widehat{E}}(x)\ \exp_{\omega_E,n}^*(z)$$

for every $x \in \hat{E}(\mathfrak{m}_n)$ and $z \in H^1(k_n, V^*(1))$. Here $\exp_{\omega_E,n}^* = \omega_E^* \circ \exp_{E,n}^*$. If there is no fear of confusion, we write $\exp_{\omega_E,n}^*(z)$ as $\exp_{\omega_E}^*(z)$. Then using the identification $\widehat{\phi} : \widehat{\mathbb{G}}_m \cong \widehat{E}$, the morphism Col_n is described in terms of the dual exponential map as follows.

$$\begin{aligned}\mathrm{Col}_n(z) &= \sum_{\sigma \in \Gamma_n} (c_n^\sigma, z)_{E,n}\, \sigma \\ &= \sum_{\sigma \in \Gamma_n} (\, \mathrm{Tr}_{k_n/\mathbb{Q}_p} \log_p(d_n^\sigma)\, \exp^*_{\omega_E}(z)\,)\, \sigma \\ &= \left(\sum_{\sigma \in \Gamma_n} \log_p(d_n^\sigma)\, \sigma \right) \left(\sum_{\sigma \in \Gamma_n} \exp^*_{\omega_E}(z^\sigma)\, \sigma^{-1} \right).\end{aligned}$$

Let G_n be the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$ and let χ be a finite character of G_{n+1} of conductor p^{n+1} which is trivial on Δ. Then we have

$$\sum_{\sigma \in \Gamma_n} \log_p(d_n^\sigma)\, \chi(\sigma) = \begin{cases} \tau(\chi) & \text{if } \chi \text{ is non-trivial,} \\ \;\; 0 & \text{otherwise} \end{cases}$$

where $\tau(\chi)$ is the Gauss sum $\sum_{\sigma \in G_{n+1}} \chi(\sigma)\, \zeta^\sigma_{p^{n+1}}$. Hence for $\chi \neq 1$, we have

$$\chi \circ \mathrm{Col}(z) = \tau(\chi) \sum_{\sigma \in \Gamma_n} \exp^*_{\omega_E}(z^\sigma)\, \chi(\sigma)^{-1}.$$

Kato showed that there exists an element $z^{\mathrm{Kato}} \in \varprojlim_n H^1(k_n, T^*(1))$ such that

$$\sum_{\sigma \in \Gamma_n} \exp^*_{\omega_E}((z^{\mathrm{Kato}})^\sigma)\, \chi(\sigma)^{-1} = e_p(\overline{\chi}) \frac{L(E, \overline{\chi}, 1)}{\Omega_E^+}$$

where $e_p(\chi)$ is the value at $s = 1$ of the p-Euler factor of $L(E, \chi, s)$, that is, $e_p(\chi) = 1$ if χ is non-trivial and $e_p(\chi) = \left(1 - \frac{1}{p}\right)$ if χ is trivial. (See [Ka], Theorem 12.5.) Hence we have

$$\chi \circ \mathrm{Col}(z^{\mathrm{Kato}}) = \tau(\chi) \frac{L(E, \overline{\chi}, 1)}{\Omega_E^+}$$

if χ is non-trivial. The p-adic L-function $L_p(E, s)$ is written of the form

$$L_p(E, s) = \mathcal{L}_{p,\gamma}(E, \kappa(\gamma)^{s-1} - 1)$$

for some power series $\mathcal{L}_{p,\gamma}(E, X) \in \mathbb{Z}_p[[X]]$. If we identify $\Lambda = \mathbb{Z}_p[[\Gamma]]$ with $\mathbb{Z}_p[[X]]$ by sending $\gamma \mapsto 1 + X$, then it satisfies an interpolation formula

$$\chi \circ \mathcal{L}_{p,\gamma}(E, X) = \tau(\chi) \frac{L(E, \overline{\chi}, 1)}{\Omega_E^+}.$$

Since an element of Λ has only finitely many zeros, we conclude that

$$\mathrm{Col}(z^{\mathrm{Kato}})(X) = \mathcal{L}_{p,\gamma}(E, X).$$

Here we denote $\mathrm{Col}(z^{\mathrm{Kato}})$ by $\mathrm{Col}(z^{\mathrm{Kato}})(X)$ to emphasis that we regard $\mathrm{Col}(z^{\mathrm{kato}})$ as a power series in $\mathbb{Z}_p[[X]]$. Note that we have $\mathbf{1} \circ \mathrm{Col}(z) = 0$ for the trivial character $\mathbf{1}$, or $\mathrm{Col}(z)(0) = 0$, namely, any Coleman power series $\mathrm{Col}(z)(X)$ for the Tate curve has a trivial zero at $X = 0$.

4. The first derivative of the Coleman map.

We compute the first derivative of the Coleman map $\mathrm{Col}(z)(X)$. By Tate's uniformization, there is an exact sequence of local Galois representations

$$0 \to T_1 \to T \to T_2 \to 0 \tag{1}$$

where $T_1 = T_p\widehat{E} \cong \mathbb{Z}_p(1)$ and $T_2 \cong \mathbb{Z}_p$. The cup product induces a non-degenerate paring

$$H^1(k_n, T_1) \times H^1(k_n, T_1^*(1)) \to H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p.$$

With the identification by $\widehat{\phi} : T_1 \cong \mathbb{Z}_p(1)$, this is in fact the cup product pairing of $\mathbb{G}_m$

$$(\ ,\ )_{\mathbb{G}_m,n} :\ H^1(k_n, \mathbb{Z}_p(1)) \times H^1(k_n, \mathbb{Z}_p) \to H^2(k_n, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p.$$

If there is no fear of confusion, we write $(\ ,\ )_{\mathbb{G}_m,n}$ simply as $(\ ,\ )_{\mathbb{G}_m}$. Since $c_n \in \widehat{E}(k_n) \subset H^1(k_n, T_1)$, we have

$$(c_n^\sigma,\ z)_{E,n} = (d_n^\sigma,\ \pi(z))_{\mathbb{G}_m,n}$$

for $z \in H^1(k_n, T^*(1))$ where π is the morphism induced by the projection $T^*(1) \to T_1^*(1)$. Tate's uniformization ϕ also induces a commutative diagram

$$\begin{tikzcd}
H^1(k_n, V^*(1)) \arrow[r, "\exp_E^*"] \arrow[d, "\pi"'] & k_n\,\omega_E \arrow[r, "\omega_E^*"] & k_n \arrow[d] \\
H^1(k_n, V_1^*(1)) \arrow[r, "\exp_{\mathbb{G}_m}^*"] & k_n\,\omega_{\mathbb{G}_m} \arrow[r, "\omega_{\mathbb{G}_m}^*"] & k_n
\end{tikzcd}$$

where $\omega_{\mathbb{G}_m}$ is the invariant differential of $\mathbb{G}_m$ which is $\frac{dX}{1+X}$ on $\widehat{\mathbb{G}}_m$, and $\omega_{\mathbb{G}_m}^*$ is the dual basis for $\omega_{\mathbb{G}_m}$. We also put $\exp_{\omega_{\mathbb{G}_m}}^* = \omega_{\mathbb{G}_m}^* \circ \exp_{\mathbb{G}_m}^*$.

Now we compute the derivative. With the same notation as the previous section, we have

$$\begin{aligned}
\mathrm{Col}_n(z) &= \sum_{\sigma\in\Gamma_n} (c_n^\sigma,\ z)_{E,n}\,\sigma = \sum_{\sigma\in\Gamma_n} (d_n^\sigma,\ \pi(z))_{\mathbb{G}_m,n}\,\sigma \\
&= \sum_{\sigma\in\Gamma_n} ((x_n^\gamma/x_n)^\sigma,\ \pi(z))_{\mathbb{G}_m,n}\,\sigma \\
&= (\gamma^{-1}-1) \sum_{\sigma\in\Gamma_n} (x_n^\sigma,\ \pi(z))_{\mathbb{G}_m,n}\,\sigma.
\end{aligned}$$

Therefore by the identification $\mathbb{Z}_p[X]/((X+1)^{p^n}-1) \cong \mathbb{Z}_p[\Gamma_n]$, $X \mapsto \gamma - 1$, we have

$$\frac{\mathrm{Col}(z)(X)}{X} \ \equiv\ -\frac{1}{\gamma} \sum_{\sigma\in\Gamma_n} (x_n^\sigma,\ \pi(z))_{\mathbb{G}_m,n}\,\sigma \mod \frac{(X+1)^{p^n}-1}{X}.$$

Hence

$$\mathrm{Col}(z)'(0) \ \equiv\ -\,(\mathrm{N}x_n,\ \pi(z))_{\mathbb{G}_m,0} \mod p^n.$$

Since $\mathrm{N}x_n = p^{e_n}\mathrm{N}(u_n) = p^{e_n}$ and by Proposition 2.2, we have

$$(\mathrm{N}x_n,\, \pi(z))_{\mathbb{G}_m} = e_n\,(p,\, \pi(z))_{\mathbb{G}_m} \equiv \frac{p}{(p-1)\log_p \kappa(\gamma)}\,(p,\, \pi(z))_{\mathbb{G}_m} \mod p^n.$$

Taking limit for n, we have that

$$\mathrm{Col}(z)'(0) = -\frac{p}{(p-1)\log_p \kappa(\gamma)}\,(p,\, \pi(z))_{\mathbb{G}_m}. \tag{2}$$

Next we compute $(p,\, \pi(z))_{\mathbb{G}_m}$. We consider the exact sequence

$$H^1(\mathbb{Q}_p, T^*(1)) \xrightarrow{\ \pi\ } H^1(\mathbb{Q}_p, T_1^*(1)) \xrightarrow{\ \delta_2\ } H^2(\mathbb{Q}_p, T_2^*(1))$$

induced by (1), and a diagram

$$\begin{array}{ccc} H^1(\mathbb{Q}_p, T_1) \times H^1(\mathbb{Q}_p, T_1^*(1)) & \xrightarrow{(\ ,\ )_{\mathbb{G}_m}} & H^2(\mathbb{Q}_p, \mathbb{Z}_p(1)) = \mathbb{Z}_p \\ {\scriptstyle \delta_1}\big\uparrow \qquad\qquad {\scriptstyle \delta_2}\big\downarrow & & \big\downarrow \\ H^0(\mathbb{Q}_p, T_2) \times H^2(\mathbb{Q}_p, T_2^*(1)) & \xrightarrow{(\ ,\ )_{\mathbb{G}_m}} & H^2(\mathbb{Q}_p, \mathbb{Z}_p(1)) = \mathbb{Z}_p. \end{array}$$

It is straightforward to see that the connecting morphism δ_1 is given by

$$H^0(\mathbb{Q}_p, T_2) = \mathbb{Z}_p \;\to\; \mathbb{Q}_p^\times \otimes \mathbb{Z}_p = H^1(\mathbb{Q}_p, T_1), \quad 1 \mapsto q_E \otimes 1.$$

Hence for $w \in H^1(\mathbb{Q}_p, T_1^*(1))$, we have

$$(q_E \otimes 1,\, w)_{\mathbb{G}_m} = (\delta_1(1),\, w)_{\mathbb{G}_m} = (1,\, \delta_2(w))_{\mathbb{G}_m}.$$

In particular, if w comes from $H^1(\mathbb{Q}_p, T^*(1))$, namely, it is of the form $\pi(z)$, then

$$(q_E \otimes 1,\, w)_{\mathbb{G}_m} = (q_E \otimes 1,\, \pi(z))_{\mathbb{G}_m} = (1,\, \delta_2 \circ \pi(z))_{\mathbb{G}_m} = 0. \tag{3}$$

On the other hand, if we put $q_E = p^{\mathrm{ord}_p(q_E)}\,\rho\, u_q$ where $\rho \in \mu_{p-1}$ and $u_q \in 1 + p\mathbb{Z}_p$, we have

$$(q_E \otimes 1,\, w)_{\mathbb{G}_m} = \mathrm{ord}_p(q_E)\;(p,\, w)_{\mathbb{G}_m} + (u_q,\, w)_{\mathbb{G}_m} \tag{4}$$

$$= \mathrm{ord}_p(q_E)\;(p,\, w)_{\mathbb{G}_m} + \log_p(u_q)\;\exp^*_{\omega_{\mathbb{G}_m}}(w). \tag{5}$$

Hence by (3) and (5) we have

$$(p,\, \pi(z))_{\mathbb{G}_m} = -\frac{\log_p(u_q)}{\mathrm{ord}_p(q_E)}\exp^*_{\omega_{\mathbb{G}_m}}(\pi(z)) = -\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\exp^*_{\omega_E}(z). \tag{6}$$

Combining (2) and (6), we obtain

Theorem 4.1. *For $z \in \varprojlim_n H^1(k_n, T^*(1))$, the first derivative of the Coleman map* $\mathrm{Col}(z)$ *is given by*

$$\frac{d}{dX}\mathrm{Col}(z)(X)\,|_{X=0} = \frac{p}{(p-1)\log_p \kappa(\gamma)}\,\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\exp^*_{\omega_E}(z).$$

Now if $E/\mathbb{Q}$ has split multiplicative reduction at p, then we may assume that E is locally the Tate curve for some $q_E \in \mathbb{Q}_p^\times$. We apply the above formula to Kato's element $z = z^{\mathrm{Kato}}$. Since $\exp^*_{\omega_E}(z^{\mathrm{Kato}}) = (1-\frac{1}{p})\frac{L(E,1)}{\Omega_E^+}$, we have

Corollary 4.2. *Let $\mathcal{L}_{p,\gamma}(E,X)$ be the power series in $\mathbb{Z}_p[[X]]$ such that $L_p(E,s) = \mathcal{L}_{p,\gamma}(E,\kappa(\gamma)^{s-1}-1)$. Then*

$$\frac{d}{dX}\mathcal{L}_{p,\gamma}(E,X)\mid_{X=0} = \frac{1}{\log_p \kappa(\gamma)}\,\frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\,\frac{L(E,1)}{\Omega_E^+},$$

or

$$\frac{d}{ds}L_p(E,s)\mid_{s=1} = \frac{\log_p(q_E)}{\mathrm{ord}_p(q_E)}\,\frac{L(E,1)}{\Omega_E^+}.$$

References

[C] P. Colmez, La conjecture de Birch et Swinnerton-Dyer p-adique, Séminaire Bourbaki - Volume 2002/2003 - Exposés 909-923 Astérisque 294 (2004)

[H] T. Honda, On the theory of commutative formal groups, J. Math. Soc. Japan 22 (1970), 213–246.

[GS] R. Greenberg and G. Stevens, p-adic L-functions and p-adic periods of modular forms, Invent. Math. 111 (1993), 2, 407-447.

[Ka] K. Kato, P-adic Hodge theory and values of zeta funcions of modular forms, Cohomologies p-adiques et applications arithmétiques (III), Astérisque 295 (2004), 117-290.

[KKT] K. Kato, M. Kurihara, T. Tsuji, Local Iwasawa theory of Perrin-Riou and syntomic complexes, preprint 1996.

[Ku] M. Kurihara, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, Invent.Math. 149 (2002), 195-224.

[Ko] S. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes, Invent. math. 152 (2003) 1, 1-36.

[MTT] B. Mazur, J. Tate, J. Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. Invent. math. 84 (1986) 1-48.

[R] K. Rubin, Euler systems and modular elliptic curves. Galois representations in arithmetic algebraic geometry (Durham, 1996), 351–367, London Math. Soc. Lecture Note Ser., 254, Cambridge Univ. Press, Cambridge, 1998.

[S1] J. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics 106, Springer-Verlag.

[S2] J. Silverman, Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Mathematics 151, Springer-Verlag.

Shinichi Kobayashi
Graduate School of Mathematics
Nagoya University
Furo-cho Chikusa-ku
Nagoya 464-8602
Japan
shinichi@math.nagoya-u.ac.jp