Pacific Journal of Mathematics

SUPERSINGULAR PRIMES AND p-ADIC L-FUNCTIONS

Luis Manuel Navas Vicente

Volume 198 No. 2 April 2001

PACIFIC JOURNAL OF MATHEMATICS
Vol. 198, No. 2, 2001

SUPERSINGULAR PRIMES AND p-ADIC L-FUNCTIONS

Luis Manuel Navas Vicente

We discuss the problem of finding a p-adic L-function attached to an elliptic curve with complex multiplication over an imaginary quadratic field K, for the case of a prime where the curve has *supersingular* reduction. While the case of primes of ordinary reduction has been extensively studied and is essentially understood, yielding many deep and interesting results, basic questions remain unanswered in the case of supersingular reduction. We will discuss a conjecture, related to another in Rubin, 1987, and some ideas related to the problem in general. The basic tools originate with the work of J. Coates and A. Wiles in 1977 and 1978, and are developed in the work of K. Rubin.

1. Set-up.

The analytic theory of L-functions and arithmetic properties of their special values goes back to the 19th-century work of Kummer on the arithmetic of cyclotomic fields. His congruences for Bernoulli numbers were re-cast more than a century later as the p-adic interpolation of Riemann's Zeta Function and Dirichlet L-series, whose known special values are basically Bernoulli numbers. Kummer himself introduced logarithmic differentiation modulo a prime p and the use of cyclotomic units as a method of uncovering the rich arithmetic structure of cyclotomic fields. In the modern theory, these classical p-adic L-functions arise as a relation between the $\mathbb{Z}_p[[t]]$-module of cyclotomic units and that of local p-adic units. The element relating them is essentially the interpolating L-function, and the precise interpolation result is obtained by a suitable logarithmic differentiation homomorphism. The theory generalizes to the arithmetic of abelian extensions of imaginary quadratic fields via the consideration of an elliptic curve as the arithmetic object. Technical complications arise at primes p which do not split in the quadratic extension, and relatively few results are known compared to the ordinary split case. The main objective of this paper is to suggest a way (§2) by which interesting two-variable p-adic L-functions may arise from an elliptic curve with CM, at primes of supersingular reduction.

The relative complexity of the method hinges on the relation between the arithmetic "elliptic" units and p-adic local units in the supersingular case,

to the author's knowledge as yet unclarified, and perhaps worthy of separate interest in itself. Propositions 2.1 and 2.2 contain preliminary suggestions on this problem. Theorem 5.5 expresses the L-values which we believe should be interpolated by a "supersingular" p-adic L-function, in terms of p-adic logarithmic derivatives on elliptic units. These are values twisted by a character of p-power order. §6 generalizes this to higher-order derivations of a two-variable formal power series, showing how the p-character and the local grossencharacter act together. Finally, Theorems 7.4 and 7.6 are local computations with logarithmic derivatives analogous to those done by Coates and Wiles in [**1**, **2**] for primes of ordinary reduction, hopefully of use to those who may wish to obtain explicit results on the p-adic growth properties of L-values, for example. We prove the relevant properties of the logarithmic differentiation homomorphisms used for these computations. The form of these results given supersingular reduction is similar to, but rather less transparent than in the ordinary case, as far as taking p-adic valuations is concerned.

Let E be an elliptic curve over an imaginary quadratic field K, with complex multiplication by the ring of integers $\mathcal{O}_K$. The following notation is standard. Let ψ be the Hecke grossencharacter attached to E, and $\mathfrak{f}$ its conductor. Pick a prime $\mathfrak{p}$ of K not dividing $6\mathfrak{f}$, and let $p \neq 2, 3$ be the prime of $\mathbb{Z}$ below $\mathfrak{p}$. Assume that p remains prime in K. This implies that E has good supersingular reduction at $\mathfrak{p}$. Let $\pi = \psi(\mathfrak{p})$. This is the unique generator of $\mathfrak{p}$ that reduces to Frobenius modulo $\mathfrak{p}$. Note that p and π differ only by a unit of $\mathcal{O}_K$.

Consider for $n \geq 0$ the abelian extensions $K(E_{\pi^{n+1}})/K$ obtained by adjoining the coordinates of the $\mathfrak{p}^{n+1}$-division points on E. Define $E_{\pi^\infty} = \bigcup_{n\geq 0} E_{\pi^{n+1}}$ and consider the Galois groups $G_n = G(K(E_{\pi^{n+1}})/K)$ $G_\infty = G(K(E_{\pi^\infty})/K)$. Denote by $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$ and by $\mathcal{O}_\mathfrak{p}$ its local ring of integers. We use the same symbol $\mathfrak{p}$ for the prime ideal of $\mathcal{O}_\mathfrak{p}$. Let $\bar{K}_\mathfrak{p}$ be a fixed algebraic closure of $K_\mathfrak{p}$. Let $K_n = K_\mathfrak{p}(E_{\pi^{n+1}})$ and $K_\infty = \bigcup_{n=0}^\infty K_n = K_\mathfrak{p}(E_{\pi^\infty})$. One has canonically $G_n = G(K_n/K_\mathfrak{p})$ and $G_\infty = G(K_\infty/K_\mathfrak{p})$. The structure of these extensions is described by the theory of Lubin-Tate formal groups. This is a very useful fact, since all Lubin-Tate formal groups over $\mathcal{O}_\mathfrak{p}$ are isomorphic and one can choose among them one well suited for computations. This idea is illustrated in [**1**, **2**].

In our case, the hypothesis of supersingular reduction is equivalent to this formal group having height 2 and not 1 as in the case of ordinary reduction.

The p-part of the grossencharacter corresponds to the character $\kappa : G_\infty \to \mathcal{O}_\mathfrak{p}^*$ which gives the action of G_∞ on p-power division points of any of the Lubin-Tate formal groups associated to π over $\mathcal{O}_\mathfrak{p}$. If $\mathcal{E}$ is such a group, then

$$\omega^\sigma = [\kappa(\sigma)](\omega) \quad \forall \omega \in \mathcal{E}_{p^\infty}, \quad \sigma \in G_\infty, \tag{1}$$

where $[\alpha]$ is the $\mathcal{O}_\mathfrak{p}$-endomorphism of $\mathcal{E}$ corresponding to $\alpha \in \mathcal{O}_\mathfrak{p}$. κ establishes isomorphisms $G_n \cong \mathcal{O}_\mathfrak{p}^*/(1+\mathfrak{p}^{n+1}\mathcal{O}_\mathfrak{p}) \cong \mu_{q-1}\times(1+\mathfrak{p}\mathcal{O}_\mathfrak{p})/(1+\mathfrak{p}^{n+1}\mathcal{O}_\mathfrak{p})$, and $G_\infty \cong \mathcal{O}_\mathfrak{p}^* \cong \mu_{q-1} \times (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p})$ where $q = p^2$ in the supersingular case. These correspond to the decompositions $G_n \cong \Delta \times \Gamma_n$ $G_\infty \cong \Delta \times \Gamma_\infty$ where $\Delta = G_0 = G(K_\mathfrak{p}(E_\mathfrak{p})/K_\mathfrak{p}), \Gamma_n = G(K_n/K_0), \Gamma_\infty = G(K_\infty/K_0)$. In the case of supersingular reduction we have $\kappa : \Gamma_\infty \cong 1 + \mathfrak{p}\mathcal{O}_\mathfrak{p} \cong \mathbb{Z}_p^2$. These are therefore Iwasawa $\mathbb{Z}_p^2$ extensions, not $\mathbb{Z}_p$ extensions as in the ordinary case, which complicates matters. We let κ_0 be the restriction of κ to $\Delta = G_0$. It establishes an isomorphism $\Delta \cong \mu_{q-1}$.

Let $\Lambda = \mathbb{Z}_p[[G_\infty]] = \varprojlim \mathbb{Z}_p[G_n]$ be the Iwasawa algebra. Let ρ be, as in [**5**], the $\mathbb{Z}_p$-representation of Δ that reduces modulo p to the $\mathbb{F}_p$-representation of Δ giving the action on $E_\mathfrak{p}$. Lemma 11.5 of [**5**] shows that this is an irreducible representation, and in the supersingular case, its degree is 2. In particular, $\Lambda^\rho = \mathcal{O}_\mathfrak{p}[[\Gamma_\infty]] \cong \mathcal{O}_\mathfrak{p}[[S,T]]$ since $\Gamma_\infty \cong \mathbb{Z}_p^2$, although the isomorphism is not canonical, depending on a choice of topological generators for Γ_∞. For this reason p-adic L-functions in the supersingular case will be 2-variable L-functions.

We need the following facts. If * denotes the action of the non-trivial automorphism of $K_\mathfrak{p}/\mathbb{Q}_p$, then $\rho \cong \kappa_0 \oplus \kappa_0{}^*$ over $K_\mathfrak{p}$ and $\kappa_0{}^* = \kappa_0{}^p$ because * gives the Frobenius element of $K_\mathfrak{p}/\mathbb{Q}_p$, and p is inert.

2. Iwasawa Structure of Local Units.

Let U_n be the group of units of K_n congruent to 1 modulo the unique prime ideal above p, and C_n the closure in K_n of the group of Robert elliptic units of K_n. One has $C_n \subseteq U_n$. Let $U_\infty = \varprojlim U_n$ and $C_\infty = \varprojlim C_n$, where the limits are with respect to the norm maps. In [**5**], Lemma 11.9, it is shown that $U_\infty^\rho \cong (\Lambda^\rho)^2$ and $C_\infty^\rho \cong \Lambda^\rho$. Furthermore, one can decompose U_∞^ρ into a direct sum

$$U_\infty^\rho = U_1 \oplus U_2 \tag{2}$$

such that $\delta(U_1) = \mathcal{O}_\mathfrak{p}$ and $\delta(U_2) = 0$, where δ is the "reciprocity law map" $\delta : U_\infty^\rho \to \mathcal{O}_\mathfrak{p}$. δ is a "κ-homomorphism," meaning $\delta(u^\sigma) = \kappa(\sigma)\delta(u) \quad \forall \sigma \in G_\infty$, and δ maps Λ^ρ-submodules of U_∞^ρ to ideals of $\mathcal{O}_\mathfrak{p}$. (See [**5**], Prop. 11.7.)

We come now to a problem of central interest. In [**8**] it was stated that one could choose a decomposition as in (2) in which C_∞^ρ would be contained in one of the two free components U_1, U_2. The truth of this statement seems still not to be known at this time. We will refer to this conjecture as (C).

If (C) is true, then a generator c of C_∞^ρ and a generator u of the free component that C_∞^ρ would lie in are related by $c = f \cdot u$, where f is an element of Λ^ρ; now f can be viewed as a power series in two variables with

coefficients in $\mathcal{O}_{\mathfrak{p}}$. This would be a natural candidate for a two-variable $\mathfrak{p}$-adic L-function, since this procedure is completely analogous to the way one-variable p-adic L-functions arise in the ordinary case and in the "classical" case over $\mathbb{Q}$.

The question (see [**8**]) would then also be to find a generator u of sufficiently explicit form that the Coates-Wiles logarithmic differentiation map and its generalizations, which yield L-values when applied to elliptic units, yield a sufficiently explicit factor when applied to u. This is what Coates and Wiles do in the ordinary case [**1**, **2**], using the basic Lubin-Tate formal group. This in turn leads to an understanding of the p-adic interpolation properties of those L-values. Over $\mathbb{Q}$ this theory gives the classical congruences of Kummer, Clausen and Von Staudt.

We study to what extent a decomposition of U_∞^ρ as in (2) can be "perturbed."

Proposition 2.1. *If $u \in U_\infty^\rho$, then*:

(i) $\delta(\Lambda^\rho u) = \mathcal{O}_{\mathfrak{p}}$ *if and only if* $\delta(u) \not\equiv 0 \bmod \pi$.

(ii) *If $u_1, u_2 \in U_\infty^\rho$ with $\Lambda^\rho u_2 \subseteq \Lambda^\rho u_1$, and $\delta(u_1), \delta(u_2) \neq 0$, then $\Lambda^\rho u_2 = \Lambda^\rho u_1$ if and only if* $\operatorname{ord}_p(\delta(u_2)) = \operatorname{ord}_p(\delta(u_1))$.

Proof. (i) is straightforward from the properties of δ. In general, $\delta(\Lambda^\rho u) = \mathcal{O}_{\mathfrak{p}}\delta(u)$. For (ii), write $u_2 = f \cdot u_1$ and apply δ. Since $\delta(u_2) = f(\kappa(\gamma_1) - 1, \kappa(\gamma_2) - 1)\delta(u_1)$, (see [**1**]), $\Lambda^\rho u_2 = \Lambda^\rho u_1$ if and only if f is a unit in Λ^ρ, and this is so if and only if $f(0,0)$ is a unit at p. Since $f(\kappa(\gamma_1) - 1, \kappa(\gamma_2) - 1) \equiv f(0,0) \bmod \pi$, we see that this is the case if and only if the quotient of $\delta(u_1), \delta(u_2)$ is a unit at p. □

Proposition 2.2. *Suppose we have $U_\infty^\rho = U_1 \oplus U_2$ with $\delta(U_2) = 0$, and hence $\delta(U_1) = \mathcal{O}_{\mathfrak{p}}$. Let $u \in U_\infty^\rho$ such that $\delta(u) \in \mathcal{O}_{\mathfrak{p}}^*$. Using additive notation, let $u = u_1 + u_2$, with $u_1 \in U_1, u_2 \in U_2$. Then $U_1 = \Lambda^\rho u_1$ and $U_\infty^\rho = \Lambda^\rho u \oplus U_2$.*

Proof. For the first part, note that $\delta(u_1) = \delta(u) \in \mathcal{O}_{\mathfrak{p}}^*$ and, since $\Lambda^\rho u_1 \subseteq U_1$, by the remarks above, equality must hold. As for the second, clearly $u_1 = u - u_2 \in \Lambda^\rho u + U_2$, therefore $U_1 \subset \Lambda^\rho u + U_2$, and hence $U_\infty^\rho = \Lambda^\rho u + U_2$. The sum is direct: If $v \in \Lambda^\rho u \cap U_2$ then $v = f \cdot u = v_2$ for some $f \in \Lambda^\rho$ and $v_2 \in U_2$. Thus $f \cdot u_1 = v_2 - f \cdot u_2 \in U_1 \cap U_2 = 0$, and so $f = 0$ and $v_2 = 0$. □

Hence if we find an element u in U_∞^ρ such that $\delta(u)$ is a unit, and we start with a given decomposition $U_\infty^\rho = U_1 \oplus U_2$, where $\delta(U_2) = 0$, then we can replace our U_1 with $\Lambda^\rho u$ (i.e., assume that U_1 is generated by u) without changing U_2. There is then a relation $c = f \cdot u + \widetilde{f} \cdot v$, where c generates C_∞^ρ, $\delta(v) = 0$ and $f, \widetilde{f}$ are two-variable power series with coefficients in $\mathcal{O}_{\mathfrak{p}}$.

A natural u having a particularly "simple" form was already used by Wiles in [**2**] for the ordinary case, and works also in the supersingular case.

The more explicit the evaluation of the Coates-Wiles derivations on u, v is, the more explicit the relation becomes.

If (C) holds, then the second term with $\tilde{f}$ and v disappears. If (C) is false, then one must also study the "extra factor" v. We know that $\delta(v) = 0$, but the generalized δ-maps need not vanish at v. The nature of these is connected with explicit reciprocity laws. If (C) is true, this would raise the further question (C′) of whether the elliptic units C_∞^ρ lie in the free component U_1 having as generator the "special" sequence of local units u discovered by Coates and Wiles, in which case we would get an explicit relation of the form $f(*,*) = (L - \text{value}) \cdot$ (explicit factors) , but this may be too good to be true. Nevertheless, see [**9**] for a different approach to this problem and evidence that in any case makes investigation of the problem interesting.

3. The Basic Lubin-Tate Formal Group.

See [**3**] for details or proofs of the following facts. The basic Lubin-Tate formal group associated to π is the formal group $\mathcal{E}$ in which multiplication by π is given by the polynomial $[\pi](X) = \pi X + X^q$. It is the simplest series over $\mathcal{O}_\mathfrak{p}$ satisfying the Lubin-Tate conditions $f(X) \equiv X \bmod X^2$ and $f(X) \equiv \pi X \bmod \mathfrak{p}$, and is simpler to work with computationally. In general we let $[\alpha]$ denote the power series representing the $\mathcal{O}_\mathfrak{p}$-endomorphism of $\mathcal{E}$ given by the action of α.

Let $\mathbf{N}_{m,n}, \mathbf{T}_{m,n}, \mathbf{N}_n, \mathbf{T}_n$ represent the norm and trace maps from K_m to K_n and from K_n to $K_\mathfrak{p}$ respectively. Let $\dot{+}$ denote addition in $\mathcal{E}$ and λ the logarithm (normalized isomorphism with the additive formal group $\mathbb{G}_a$).

We fix a generator (ω_n) of the Tate module, that is, a sequence with ω_n in the ring of integers of K_n such that $[\pi](\omega_{n+1}) = \omega_n$ for all $n \geq 0$. Then $K_n = K_\mathfrak{p}(\omega_n)$ and in fact this sequence is also norm compatible: $N_{n+1,n}(\omega_{n+1}) = \omega_n$.

If $u = (u_n)_{n\geq 0} \in U_\infty$, denote by g_u the Coleman power series associated to u, that is, the unique series $g_u \in \mathcal{O}_\mathfrak{p}[[T]]^*$ such that $g_u(\omega_n) = u_n$ for all $n \geq 0$. For σ in G_∞, given the definition of κ, we have the relation $g_{u^\sigma} = g_u \circ [\kappa(\sigma)]$.

4. L-values.

Over the complex numbers $\mathbb{C}$, special values of Hecke L-functions at the integers may be expressed as logarithmic derivatives of theta functions. One may obtain an analogous p-adic relationship. Details of these facts may be found in [**6**], which draws from [**1**, **2**]. To get L-values, one uses the Robert elliptic units, which are defined by picking a suitable theta function Θ. One can find a sequence $c = (c_n)$ of elliptic units whose projection onto the ρ-eigenspace generates C_∞^ρ over the Iwasawa algebra Λ. ([**6**] Theorem 12.11.)

Let Φ be the Coleman power series corresponding to c. Let Ω be an $\mathcal{O}_K$-generator for the period lattice of a suitable Weierstrass model of $E/\mathbb{C}$. The central relation is contained in the following result of Rubin [**6**], §12.

Theorem 4.1. *Let $Q \in E(\bar{K})$ be of exact order $\mathfrak{f}\mathfrak{p}^{n+1}$. Then for $k \geq 1$, and χ a character of G_n of p-power order,*

$$\sum_{\sigma \in G_n} \chi(\sigma) \mathcal{D}^k \log \Phi^\sigma\big|_{T=\omega_n{}^\sigma} = \sum_{\sigma \in G_n} \chi(\sigma) \left(\frac{d}{dz}\right)^k \log \Theta(z)|_{z=Q^\sigma}$$
$$= B \cdot \pi^{n+1} \cdot \Omega^{-1} L_{\mathfrak{f}\mathfrak{p}} \left(\bar{\psi}^k \chi, k\right)$$

where $\mathcal{D}f = \frac{1}{\lambda'} \frac{f'}{f}$ is the Coates-Wiles logarithmic derivation ([**9**], §2) *and $B = B_k$ may be chosen to be a unit over p, at least for $1 \leq k \leq q-1$.*

5. Formal logarithmic derivatives.

Definition 5.1. Let $\mathcal{L}$ denote the "formal logarithmic derivative" on $\mathcal{O}[[T]]$, given by $\mathcal{L}f = \frac{1}{\lambda'(T)} D \log(f) = \frac{1}{\lambda'(T)} \frac{f'}{f}$ for f in $\mathcal{O}[[T]]$.

It is easily seen to satisfy $\mathcal{L}f_1 f_2 = \mathcal{L}f_1 + \mathcal{L}f_2$ for $f_1, f_2 \in \mathcal{O}[[T]]$ and $\mathcal{L}(f \circ [\alpha]) = \alpha \cdot (\mathcal{L}f \circ [\alpha])$ for $f \in \mathcal{O}[[T]]$ and $\alpha \in \mathcal{O}_\mathfrak{p}$.

Definition 5.2. Let $u = (u_n)_{n \geq 0} \in U_\infty$, and define $\delta_m(u) = \pi^{-m} \mathbf{T}_m \mathcal{L} g_u(\omega_m)$. Then $\delta_m(u) = \delta_n(u)$ for all $m, n \geq 0$. Let $\delta(u)$ be the common value.

Lemma 5.3. *We have $\delta(u) = (\pi - 1)\mathcal{L}g_u(0)$ for all $n \geq 0$. Thus $\delta(u) \in \mathcal{O}_\mathfrak{p}$.*

Proof. See [**3**], §8. □

Definition 5.4. For a character χ of G_n, taking values in $\bar{K}_\mathfrak{p}{}^*$, define a map $\delta_{n,\chi} : U_\infty \to \bar{K}_\mathfrak{p}$ by the formula $\delta_{n,\chi}(u) = \sum_{\sigma \in G_n} \chi(\sigma) \mathcal{L} g_u(\omega_n^\sigma)$.

We list the basic properties of the maps $\delta_{n,\chi}$ from [**9**], §2, and some others.

1) $\delta_{n,\chi}(u_1 \cdot u_2) = \delta_{n,\chi}(u_1) + \delta_{n,\chi}(u_2)$ for $u_1, u_2 \in U_\infty$.
2) By continuity, $\delta_{n,\chi}(u^a) = a \delta_{n,\chi}(u)$ if $a \in \mathcal{O}_\mathfrak{p}$.
3) If $\chi = 1$, then $\delta_{n,\chi} = \pi^n \delta$.
4) If χ is a character of G_n, and τ is any element of G_∞, then lifting χ to G_∞, one has $\delta_{n,\chi}(u^\tau) = \kappa \chi^{-1}(\tau) \delta_{n,\chi}(u)$.
5) Let γ_1, γ_2 be $\mathbb{Z}_p$-generators of Γ_∞. Then for all χ of p-power order, $u \in U_\infty^\rho$ and $f \in \Lambda^\rho$, $\delta_{n,\chi}(f \cdot u) = f\big(\kappa\chi^{-1}(\gamma_1) - 1, \kappa\chi^{-1}(\gamma_2) - 1\big)\delta_{n,\chi}(u)$ (this is slightly different from [**9**] but is proved similarly using that the character values are congruent to 1 modulo the prime above $\mathfrak{p}$ in $\bar{K}_\mathfrak{p}$).

In light of this definition and 4.1 we have the following:

Theorem 5.5. *For $n \geq 0$, $\delta_{n,\chi}(c) = B \cdot \pi^{n+1} \cdot \Omega^{-1} L_{\mathfrak{g}\mathfrak{p}}(\bar{\psi}\chi, 1)$, where B is a p-unit.*

We determine the action of $\delta_{n,\chi}$ on an element in the ρ-eigenspace U_∞^ρ and prove some additional properties of these maps. If u is any element in U_∞, let u^ρ denote the ρ-component of u in U_∞^ρ. Note $\mathrm{Tr}(\rho) = \kappa_0 + \kappa_0{}^* = \kappa_0 + \kappa_0^p$.

Proposition 5.6. *If $\chi \in \widehat{G_n}$ and $\chi = 1$ on Δ, then $\delta_{n,\chi}(u^\rho) = \delta_{n,\chi}(u)$.*

Proof.

$$\begin{aligned}\delta_{n,\chi}(u^\rho) &= \delta_{n,\chi}\left(u^{\frac{1}{q-1}\sum_{\sigma\in\Delta}\mathrm{Tr}(\rho(\sigma^{-1}))\sigma}\right)\\ &= \frac{1}{q-1}\sum_{\sigma\in\Delta}\kappa_0\chi^{-1}(\sigma)\left(\kappa_0{}^{-1}(\sigma)+\kappa_0{}^{-p}(\sigma)\right)\delta_{n,\chi}(u)\\ &= \frac{1}{q-1}\left(\sum_{\sigma\in\Delta}\chi^{-1}(\sigma)+\sum_{\sigma\in\Delta}\chi^{-1}\kappa_0{}^{1-p}(\sigma)\right)\delta_{n,\chi}(u).\end{aligned}$$

From the above we see that

$$\delta_{n,\chi}(u^\rho) = \begin{cases}\delta_{n,\chi}(u) & \text{if } \chi = 1 \text{ or } \kappa_0^{1-p} \text{ on } \Delta\\ 0 & \text{otherwise.}\end{cases} \tag{3}$$

□

Note that the condition $\chi = 1$ on Δ is equivalent to χ having p-power order, and in fact to really being a character on Γ_n. This is clear from the decomposition $G_n \cong \Delta \times \Gamma_n$ and $\#\Delta = p^2 - 1, \#\Gamma_n = p^{2n}$. From now on, let us assume that the characters χ have p-power order.

Proposition 5.7. *Let $\Gamma_{m,n} = G(K_m/K_n)$ for $m \geq n$. If $\chi \in \Gamma_{m,n}^\perp$ (i.e., $\chi = 1$ on $\Gamma_{m,n} \subseteq \Gamma_n$), then $\delta_{m,\chi} = \pi^{m-n}\delta_{n,\chi}$.*

Proof. Using the basic properties of $\mathcal{L}$ and g_u as in [**3**],

$$\begin{aligned}\delta_{m,\chi}(u) &= \sum_{\sigma\in\Gamma_m/\Gamma_{m,n}}\sum_{\tau\in\Gamma_{m,n}}\chi(\sigma\tau)\mathcal{L}g_u(\omega_m^{\sigma\tau})\\ &= \sum_{\sigma\in\Gamma_m/\Gamma_{m,n}}\chi(\sigma)\sum_{\tau\in\Gamma_{m,n}}\mathcal{L}g_u(\omega_m^\tau)^\sigma\\ &= \sum_{\sigma\in\Gamma_m/\Gamma_{m,n}}\chi(\sigma)\left(\mathbf{T}_{m,n}\mathcal{L}g_u(\omega_m)\right)^\sigma\\ &= \pi^{m-n}\sum_{\sigma\in\Gamma_n}\chi(\sigma)\mathcal{L}g_u(\omega_n^\sigma)\\ &= \pi^{m-n}\delta_{n,\chi}(u).\end{aligned} \tag{4}$$

□

Corollary 5.8. *For $\chi \in \hat{\Gamma}_{n+1}$, $\delta_{n+1,\chi^p} = \pi\delta_{n,\chi^p}$.*

Proof. From the structure of the local extensions K_n one sees immediately that $\Gamma_{n+1,n}^{\perp}$ is the subgroup of p-th powers. It follows that for any $\chi \in \hat{\Gamma_{n+1}}$, we have $\chi^p \in \Gamma_{n+1,n}^{\perp}$, and so we can view χ^p as a character of Γ_n. □

Thus in calculations we can assume that the character χ has maximum order.

6. Higher Derivatives.

We may easily generalize the maps $\delta_{n,\chi}$ so that we obtain information concerning the values $L_{\mathfrak{fp}}(\bar{\psi}^k\chi, k)$.

Definition 6.1. For $u \in U_\infty, n \geq 0, k \geq 1$, define

$$\delta_{n,\chi}^k(u) = \sum_{\sigma \in G_n} \chi(\sigma)\mathcal{D}^{k-1}\mathcal{L}g_u(\omega_n^\sigma),$$

where $\mathcal{D}$ is the derivation $\frac{1}{\lambda'(X)}\frac{d}{dx}$.

By Theorem 4.1, we have $\delta_{n,\chi}^k(c) = \pi^{n+1} \cdot B \cdot \Omega^{-1} L_{\mathfrak{fp}}(\bar{\psi}^k\chi, k)$, where B is a unit, if $1 \leq k \leq q-1$. In his paper [**4**], Katz has shown that a family of derivations $\mathcal{D}_n$ may be defined by the formula $f(X \dot{+} Y) = \sum_{n=0}^{\infty} \mathcal{D}_n f(X) Y^n$ and in addition, if $0 \leq m \leq q-1$, then $\mathcal{D}_m = \frac{1}{m!}\mathcal{D}^m$. Since $g_u \equiv 1 \mod (\pi, X), \log g_u$ converges formally, and we may write $\mathcal{D}^{k-1}\mathcal{L} = \mathcal{D}^k \log$. Substituting $f = \log g_u$ above gives $\log g_u(t \dot{+} s) = \sum_{k=0}^{\infty} \mathcal{D}_k \log g_u(t) s^k$. We may then define a power series, given a character χ of G_n and a sequence of units $u \in U_\infty$, by

$$\begin{aligned} g(u, \chi, t, s) &= \sum_{\sigma \in G_n} \chi(\sigma) \log g_u([\kappa(\sigma)](t) \dot{+} s) \\ &= \sum_{k=0}^{\infty} \left(\sum_{\sigma \in G_n} \chi(\sigma)(\mathcal{D}_k \log g_u) \circ [\kappa(\sigma)](t) \right) s^k. \end{aligned}$$

It is readily seen from the above remarks that

$$\delta_{n,\chi}^k(u) = \left(\frac{d}{ds}\right)^k g(u, \chi, \omega_n, s)\big|_{s=0} \text{ if } 1 \leq k \leq q-1.$$

In particular, $g(c, \chi, \omega_n, s)$ yields L-values.

7. Special Local Units.

As was done in [**2**] for the ordinary case, we now describe a sequence of local units which will give elements of U_∞ with simple Coleman power series. As usual, $q = p^2$. Let β in $\mathcal{O}_{\mathfrak{p}}$ be such that $\beta^{q-1} = 1-\pi$ and $\beta \equiv 1 \mod \pi$. Such a β exists by Hensel's Lemma applied to the polynomial $f(X) = X^{q-1} - (1-\pi)$. If ζ is any one of the $q-1$ roots of unity in $K_{\mathfrak{p}}$, then $f(\zeta) = \pi \equiv 0 \mod \mathfrak{p}$

and $f'(\zeta) = (q-1)\zeta^{-1} \not\equiv 0 \mod \mathfrak{p}$, so that there is a lifting of ζ to a root in $\mathcal{O}_{\mathfrak{p}}$.

Lemma 7.1. $\mathbf{N}_{K_{n+1}/K_n}(\beta - \omega_{n+1}) = (\beta - \omega_n)$ *for all* $n \geq 0$.

Proof. The minimal polynomial of ω_{n+1} over K_n is $P(X) = X^q + \pi X - \omega_n$, and hence the minimal polynomial of $\beta - \omega_{n+1}$ over K_n is $-P(\beta - X)$. It follows that $N_{n+1,n}(\beta - \omega_{n+1}) = -(-1)^q P(\beta) = P(\beta) = \beta^q + \pi\beta - \omega_n = \beta - \omega_n$. □

Theorem 7.2. *For each* d *dividing* $q-1$, *we have* $N_{n+1,n}(\beta^d - \omega_{n+1}^d) = (\beta^d - \omega_n^d)$.

Proof. The lemma is valid for any β such that $\beta^{q-1} = \pi$, in particular with β changed to $\zeta\beta$ where $\zeta^{q-1} = 1$. Taking the product over $\zeta^d = 1$ gives the result. □

We obtain a sequence of units $u^{(d)} = (u_n^{(d)}) \in U_\infty$ for $d|q-1$ whose Coleman power series is $\beta^d - X^d$.

Corollary 7.3. $\delta(u^{(d)}) = 0$ *if* $d \neq 1$. $\delta(u^{(1)}) = (1-\pi)\beta^{-1} \not\equiv 0 \bmod \pi$.

Proof. Explicit calculation, using Lemma 5.3. □

Theorem 7.4. $u^{(d)\rho} = 1$ *unless* $d = 1$.

Proof. We calculate the Coleman power series of the projections. First we compute the ρ-part of the unit $u^{(d)} = (u_n^{(d)})$:

$$u_n^{(d)\rho} = \prod_{\sigma\in\Delta} u_n^{(d)\,\frac{1}{q-1}\mathrm{Tr}(\rho(\sigma^{-1}))\sigma} = \prod_{\sigma\in\Delta} (\beta^d - \kappa_0^d(\sigma)\omega_n^d)^{\frac{1}{q-1}\mathrm{Tr}(\rho(\sigma^{-1}))}.$$

We have used the fact that $[\kappa_0(\sigma)](X) = \kappa_0(\sigma)X$ in the basic Lubin-Tate formal group. The Coleman power series for $u^{(d)\rho}$ must then be

$$\mathcal{G}(X) = \prod_{\sigma\in\Delta} (\beta^d - \kappa_0^d(\sigma)X^d)^{\frac{1}{q-1}\mathrm{Tr}(\rho(\sigma^{-1}))}.$$

Note that $\frac{1}{q-1}\mathrm{Tr}(\rho(\sigma^{-1}))$ is an element of $\mathbb{Z}_p$ and that $\beta^d - \kappa_0^d(\sigma)X^d \equiv 1 \bmod (\pi, X)$, so this expression indeed defines a power series in $\mathcal{O}_{\mathfrak{p}}[[X]]$, satisfying $\mathcal{G}(\omega_n) = {u_n}^{e(\rho)}$ for all $n \geq 0$. Furthermore, $\mathcal{G}(X) \equiv 1 \bmod (\pi, X)$. Writing $(\beta^d - \kappa_0^d(\sigma)X^d) = \beta^d \cdot (1 - (\kappa_0(\sigma)X/\beta)^d)$ we compute

$$\log \mathcal{G}(X) = \sum_{\sigma\in\Delta} \frac{1}{q-1}\mathrm{Tr}\rho(\sigma^{-1}) \log_p(\beta^d) + \sum_{\sigma\in\Delta} \frac{1}{q-1}\mathrm{Tr}\rho(\sigma^{-1}) \log\left(1 - \frac{\kappa_0^d(\sigma)}{\beta^d}X^d\right)$$

where $\log_p$ is the p-adic logarithm, and the logarithm of a power series which is congruent to 1 modulo (π, X) is given by the usual series expansion for $\log(1+X)$. Then

$$\log \mathcal{G}(X) = -\sum_{\sigma\in\Delta} \frac{1}{q-1}\mathrm{Tr}\rho(\sigma^{-1}) \sum_{k=1}^{\infty} \frac{\kappa_0^{dk}(\sigma)}{\beta^{dk}} \frac{X^{dk}}{k} \tag{5}$$
$$= -\sum_{k=1}^{\infty} \left(\frac{1}{q-1} \sum_{\sigma\in\Delta} \mathrm{Tr}\rho(\sigma^{-1}) \kappa_0^{dk}(\sigma) \right) \frac{X^{dk}}{k\beta^{dk}}.$$

We have $\mathrm{Tr}\rho(\sigma^{-1})\cdot\kappa_0^{dk}(\sigma) = \left(\kappa_0(\sigma^{-1}) + \kappa_0^*(\sigma^{-1})\right)\kappa_0^{dk}(\sigma)$ and, since $\kappa_0^* = \kappa_0^p$, when we sum over Δ the result is $\sum_{\sigma\in\Delta}(\kappa_0^{dk-1}(\sigma) + \kappa_0^{dk-p}(\sigma))$, which is 0 unless $dk - 1 \equiv 0 \bmod q-1$ or $dk - p \equiv 0 \bmod q-1$, in which cases it is equal to $q-1$. However, since $d|q-1$, we see that unless $d = 1$ these congruences are impossible, and hence $\log \mathcal{G}(X) = 0$, so that $\mathcal{G}(X) = 1$ and thus u^d projects trivially. □

For $d = 1$, we have $\log \mathcal{G}(X) = -\sum_{k\equiv 1, p \bmod q-1} X^k/k\beta^k$. It is easy to compute

$$\mathcal{Q} = \mathcal{L}\mathcal{G} = \frac{1}{\lambda'(X)}\frac{d}{dx}\log \mathcal{G}(X) = -\frac{1}{\lambda'(X)} \sum_{k\equiv 1,p} \frac{X^{k-1}}{\beta^k}$$
$$= -\frac{1}{\lambda'(X)}\beta^{-1} \sum_{k\equiv 0, p-1} \frac{X^k}{\beta^k}.$$

Compare this to the result in the ordinary case in [**1**, **2**]. We may sum the series,

$$\mathcal{Q}(X) = -\frac{1}{\lambda'(X)}\beta^{-1}\left(1 + \left[\frac{X}{\beta}\right]^{p-1}\right) \frac{1}{1 - \dfrac{X^{q-1}}{1-\pi}}.$$

We could further modify this, by employing the definition of β and the formula $(1 - X^{2ma})(1 + X^a)^{-1} = \sum_{n=0}^{2m-1}(-1)^n X^{an}$. This gives

$$\mathcal{Q}(X) = -\frac{1}{\lambda'(X)} \cdot \frac{\beta^{-1}}{1 - \left(\frac{X}{\beta}\right)^{p-1} + \left(\frac{X}{\beta}\right)^{2(p-1)} + \cdots - \left(\frac{X}{\beta}\right)^{p(p-1)}}.$$

Note that $\delta_{n,\chi}(u^\rho) = \sum_{\sigma\in G_n} \chi(\sigma)\mathcal{Q}(\omega_n^\sigma)$, although this does not simplify the expression $\delta_{n,\chi}(u^\rho) = \delta_{n,\chi}(u) = -\sum_{\sigma\in G_n}\chi(\sigma)\frac{1}{\lambda'(\omega_n{}^\sigma)}\cdot\frac{1}{\beta-\omega_n{}^\sigma}$. We compute $\lambda'(\omega_n)$.

Lemma 7.5. *For all $n \geq 0$, we have* $\lambda'(\omega_n) = \prod_{k=0}^{n} \left(1 + \frac{q}{\pi}{\omega_k}^{q-1}\right)$.

Proof. By differentiating the relation $\lambda \circ [\pi^{n+1}](X) = \pi^{n+1}\lambda(X)$ we obtain $[\pi^{n+1}]'(X)\lambda' \circ [\pi^{n+1}] = \pi^{n+1}\lambda'(X)$. Substitute $X = \omega_n$ and $\lambda'(0) = 1$ to get $[\pi^{n+1}]'(\omega_n) = \pi^{n+1}\lambda'(\omega_n)$. If f is a function and $f_n = f \circ \overset{\text{n times}}{\circ} f$ then $f_m'(X) = \prod_{n=0}^{m-1} f'(f_n(X))$ for every $m \geq 1$. Applying this to $f = [\pi]$ gives

$$[\pi^{n+1}](\omega_n) = \prod_{k=0}^{n} [\pi]'([\pi^k](\omega_n)) = \prod_{k=0}^{n} [\pi]'(\omega_{n-k}) = \prod_{k=0}^{n} [\pi]'(\omega_k).$$

Since $[\pi]'(X) = \pi + qX^{q-1}$ we conclude

$$\lambda'(\omega_n) = \pi^{-(n+1)}[\pi^{n+1}]'(\omega_n) = \pi^{-(n+1)} \prod_{k=0}^{n} (\pi + q\omega_k^{q-1}) = \prod_{k=0}^{n} \left(1 + \frac{q}{\pi}{\omega_k}^{q-1}\right).$$

□

We finish by mentioning a connection to sums $S_n(\chi, k) = \sum_{\sigma \in \Gamma_n} \chi(\sigma)(\omega_n^\sigma)^k$. A straightforward calculation gives:

Theorem 7.6. *Let $\lambda'(X)^{-1} = \sum_{i=0}^{\infty} b_i X^{(q-1)i}$, with $b_i \in \mathcal{O}_\mathfrak{p}$. Then $\delta_{n,\chi}(u^\rho) = (1-q)\beta^{-1} \sum_{m=0}^{\infty} c_m S_n(\chi, (q-1)m)$, where $c_m = \sum_{i+j=m} \frac{b_i}{(1-\pi)^j}$.*

References

[1] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Inventiones Mathematicae, **39** (1977), 223-251.

[2] ———, *On p-adic L-functions and elliptic units*, J. Aust. Math. Soc., **26**, (1978) 1-25.

[3] K. Iwasawa, *Local Class Field Theory*, Oxford University Press (1986).

[4] N. Katz, *Divisibilities, congruences, and Cartier duality*, J. Fac. Sci. Univ. Tokyo, **28** (Sec 1a) (1982), 667-678.

[5] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Inventiones Mathematicae, **103** (1991), 25-68.

[6] ———, *Tate-Shafarevitch groups and L-functions of elliptic curves with complex multiplication*, Inventiones Mathematicae, **89** (1987), 527-560.

[7] ———, *Congruences for special values of L-functions of elliptic curves with complex multiplication*, Inventiones Mathematicae, **71** (1983), 339-368.

[8] ———, *Iwasawa Theory and Elliptic Curves: Supersingular Primes*, Journées Arithmétiques, 1980, London Math. Soc. LN series, **56**.

[9] ———, *Local units, elliptic units, Heegner points and elliptic curves*, Inventiones Mathematicae, **88** (1987), 405-422.

[10] A. Wiles, *Higher explicit reciprocity laws*, Ann. Math., **107** (1978), 235-254.

Received July 20, 1999.

Departamento de Matemáticas
Universidad de Salamanca
Plaza de la Merced, 1-4
37008 Salamanca Spain
E-mail address: navas@gugu.usal.es