Advanced Studies in Pure Mathematics 17, 1989
Algebraic Number Theory — in honor of K. Iwasawa
pp. 55–72

Anderson-Ihara Theory: Gauss Sums and Circular Units

R. F. Coleman

Thrice the brinded cat hath mewed,
Thrice and once the hedge pig whined,
Harpier cries. 'tis time, 'tis time.

The Three Witches
Macbeth, Act IV Scene

Dedicated to Iwasawa on the occasion of his seventieth birthday

A few years ago, Ihara, [I], discovered a new sort of power series connected with the action of G_Q on the Tate-modules of Fermat curves of l-power degree. Since then Anderson, [A], refined and generalized these power series, interpreting them as analogues of the classical beta function. Moreover, once this analogy was made he naturally was forced to factor them into a product of three "gamma functions."

The previous paragraph is purposely vague and oversimplified. In this article I will attempt to make some of it a little less vague and indicate how the theory of these "gamma" and "beta" functions may be connected with and applied to other aspects of cyclotomy.

I. Ihara's "Beta" series

Let X_n denote the projective plane curve over Q determined by the homogeneous equation:

$$X^{l^n}+Y^{l^n}+Z^{l^n}=0.$$

Let J_n denote the Jacobian of X_n. We have natural maps, $X_{n+1}\to X_n$ and corresponding maps on the Jacobians. Hence we may define the G_Q-module

$$T=\varprojlim T_l(J_n(\bar{Q})).$$

Received December 21, 1987.
This paper is based on lectures given in Tokyo in October, 1985 and at MSRI for the conference on Iwasawa Theory in January, 1987.

Now, let Λ denote the ring

$$\boldsymbol{Z}_l[[(R-1),(S-1),(T-1)]]/(RST-1)$$

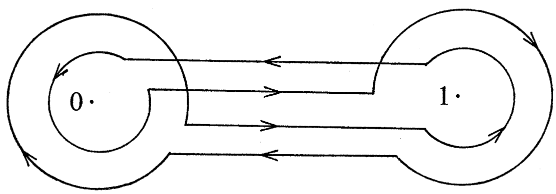
Fix a generator (ζ_n) of $T_l(\boldsymbol{G}_m)$. We can now make Λ act on $\boldsymbol{T}$, as follows: We first make R, S and T act on X_n for each n, by setting,

$$\begin{array}{ll} R & (\zeta_n X, Y, Z) \\ S\colon (X, Y, Z) \longmapsto & (X, \zeta_n Y, Z) \\ T & (X, Y, \zeta_n Z). \end{array}$$

We now use functoriality, linearity and continuity to make Λ act on $\boldsymbol{T}$.

Theorem A (Ihara). *$\boldsymbol{T}$ is a principal Λ-module.*

Moreover, if we fix an embedding of $\bar{\boldsymbol{Q}}$ in $\boldsymbol{C}$ (which we will do for the rest of this article), there is a nice choice of basis for $\boldsymbol{T}$, η, coming from the Pochhammer contour. (See Whittaker and Watson, 12.43.)



and the comparison theorem between singular and étale cohomology. (The Pochhammer contour is the commutator of the loops around 0 and 1, so it lifts to the Fermat curves which are Abelian coverings of $\boldsymbol{P}^1$ branched at $\{0, 1, \infty\}$.) Hence, for $\sigma \in G_{\boldsymbol{Q}}$, we may define an element $F_\sigma(R, S, T)$ of Λ, by the following formula:

$$F_\sigma(R, S, T)\eta = \sigma\eta.$$

Remark. Already one sees relations between F_σ and the classical Beta function. To bring the two closer together Anderson first considers F_σ as an element of $\boldsymbol{Z}_l[[\boldsymbol{Z}_l(1)\times\boldsymbol{Z}_l(1)]]$, and so a function on $\boldsymbol{Q}_l/\boldsymbol{Z}_l\times\boldsymbol{Q}_l/\boldsymbol{Z}_l$, (which among other things eliminates the choice of (ζ_n)), and then replaces the Pochhammer contour with the unit interval (this requires the use of one-motives); recall that the classical beta function is really a function of $\boldsymbol{Q}/\boldsymbol{Z}\times\boldsymbol{Q}/\boldsymbol{Z}$ and is defined by integrating over the unit interval. This is about all I want to say about the analogies except to say that the classical beta function is connected with complex de Rham cohomology, the Anderson-Ihara beta function is connected with étale cohomology and the

Morita beta-function is connected with crystalline cohomology.

For simplicity, here and for the next few sections we will suppose $l\neq 2$. As an immediate consequence of the definition and what one already knows about the action of $G_{Q(\zeta_n)}$ on $T_l(J_n)$, we have:

Theorem B (Ihara). *Suppose $a+b+c=0$. Let $\mathfrak{p}$ be a prime of $\bar{Q}$ with residue characteristic $p\neq l$. Let σ denote any element in the Frobenius coset at $\mathfrak{p}$. Let $\mathfrak{p}_n$ denote the restriction of $\mathfrak{p}$ to $Q(\zeta_n)$ and p^{f_n} the order of $F_{\mathfrak{p}_n}$. Then*

$$\prod_{i=1}^{f_n} F_\sigma(\zeta_n^{ap^i}, \zeta_n^{bp^i}, \zeta_n^{cp^i})=(1-N(\mathfrak{p}_n))^{-1}\sum_{\substack{x+y+z=0\\ x,y,z\in F_{\mathfrak{p}_n}}}\left(\frac{x}{\mathfrak{p}_n}\right)^a\left(\frac{y}{\mathfrak{p}_n}\right)^b\left(\frac{z}{\mathfrak{p}_n}\right)^c$$

where $\left(\frac{x}{\mathfrak{p}_n}\right)=\left(\frac{x}{\mathfrak{p}_n}\right)_{l^n}$ *is the l^n-th power residue symbol of x at $\mathfrak{p}_n$.*

Note that the expression on the right is a Jacobi sum which equals the product of three Gauss sums divided by the norm of $\mathfrak{p}_n$ (see below). Since $\sigma\mapsto F_\sigma$ is a one co-cycle we can also write the expression on the left as $F_{\sigma^{f_n}}(\zeta_n^a, \zeta_n^b, \zeta_n^c)$. Moreover, σ^{f_n} is a Frobenius element above $\mathfrak{p}_n$.

From the various symmetries involved, one can see that F_σ is symmetric in R, S and T. Using this and other elementary properties of F_σ one can show that if $\sigma\in G_{Q(\mu_{l^\infty})}$, then

$$F_\sigma(R, S, T)=\exp\left(\sum_{\substack{m\geq 3\\ m\text{ odd}}} b_m(\sigma)\frac{U^m+V^m+W^m}{m!}\right)$$

for some $b_m(\sigma)\in Z_l$, where $\exp(U)=R$, $\exp(V)=S$ and $\exp(W)=T$. In particular,

$$F_\sigma(R^{-1}, S^{-1}, T^{-1})=F_\sigma(R, S, T)^{-1}. \tag{1.1}$$

Ihara conjectured the following formula for these $b_m(\sigma)$ when $\sigma\in G_{Q(\mu_{l^\infty})}$:

Theorem C. *Suppose $m\geq 3$, then*

$$\zeta_n^{b_m(\sigma)(1-l^{m-1})}=c_{n,m}^{(\sigma-1)/l^n}$$

where

$$c_{n,m}=\prod_{a}{}_n\,(\zeta_n^{-a/2}-\zeta_n^{a/2})^{a^{m-1}}.$$

Here and in the following, the subscript n indicates summation or product over indices from 1 to l^n prime to l. We will prove this in § III.

Remarks. Ihara's conjecture now has at least two additional proofs together with generalizations; one due to Anderson [A] and one due to Ihara-Kaneko-Yukinari [IKY].

II. Stickelberger's and Iwasawa's Theorems

Let

$$\begin{aligned}
G_n &=: \operatorname{Gal}(\boldsymbol{Q}(\mu_{l^n})/\boldsymbol{Q}) \\
G &=: \varprojlim G_n \\
A &=: \varprojlim \boldsymbol{Z}_l[G_n] = \boldsymbol{Z}_l[[G]] \\
\chi &=: \text{the } l\text{-adic cyclotomic character} \\
\sigma_a &=: \chi^{-1}(a) \\
\theta_n &=: \sum\nolimits_n \left(\frac{a}{l^n} - \frac{1}{2}\right)\sigma_a^{-1} \\
\theta'_n &=: \sum\nolimits_n \frac{a}{l^n}\sigma_a^{-1} \\
\theta &=: \varprojlim \theta_n \in \varprojlim \boldsymbol{Q}[G_n] \subseteq \boldsymbol{Q}_l[[G]].
\end{aligned}$$

We may extend χ to a homomorphism from A to $\boldsymbol{Z}_l$ by linearity and continuity. Let I denote the kernel of this homomorphism. We have the Stickelberger ideal:

$$\mathscr{S} =: I\theta \subseteq A.$$

Also A acts naturally on the principal units, U_n, in $\boldsymbol{Z}_l[\mu_{l^n}]$. For $\mathfrak{p}$ a prime of $\boldsymbol{Q}(\mu_{l^n})$ of residue characteristic $p \neq l$, and $\psi\colon \boldsymbol{F}_p \xrightarrow{\sim} \mu_p(\overline{\boldsymbol{Q}})$, set

$$g(\mathfrak{p}, \psi) = -\sum_{x \in \boldsymbol{F}_\mathfrak{p}} \left(\frac{x}{\mathfrak{p}}\right)_{l^n}^{-1} \psi(T_{\boldsymbol{F}_\mathfrak{p}/\boldsymbol{F}_p} x).$$

We extend the action of G to $\boldsymbol{Q}(\mu_{pl^\infty})$ by making G act trivially on μ_p. We have the following perverse formulation of:

Stickelberger's Theorem (2.1). *With notation as above, suppose* $(\alpha) = \mathfrak{p}^m$, *for some* $m \in \boldsymbol{Z}$, $\alpha \in \boldsymbol{Q}(\mu_{l^n})$ *and* $\omega \in I \cap \boldsymbol{Z}[[G]]$. *Then after embedding in* $\boldsymbol{Q}_l(\mu_{l^n})$

$$\alpha^{\omega\theta'_n} = g(\mathfrak{p}, \psi)^{m\omega} \times \textit{an } l^n\textit{-th root of unity}.$$

(Note: $N\mathfrak{p}^m$ equals the norm of α to $\boldsymbol{Q}$ so is a principal unit in $\boldsymbol{Q}_l$ and so its square root makes sense as a principal unit.) See Theorem 4.2 of [L]§ 4.

To state Iwasawa's theorem we need more notation.

$U_n =:$ the principal units in $\boldsymbol{Z}_l[\mu_{l^n}]$

$V_n =:$ the l-adic completion of $\boldsymbol{Q}_l[\mu_{l^n}]^*$

$\mathscr{C}_n =:$ the subgroup of $\boldsymbol{Q}(\mu_{l^n})^*$ generated by $\{1-\zeta\colon \zeta \in \mu_{l^n}, \zeta \neq 1\}$

$\overline{\mathscr{C}}_n =:$ closure of the image of $\mathscr{C}_n$ in V_n

$U_\infty =: \varprojlim U_n$

$V_\infty =: \varprojlim V_n$

$\mathscr{C}_\infty =: \varprojlim \overline{\mathscr{C}}_n$

Finally, we have the continuous automorphisms of A:

$$\omega \longmapsto \omega^*, \text{ which is determined by } \sigma_a^* = \sigma_a^{-1}$$

and

$$\omega \longmapsto \omega(k),\ k \in \boldsymbol{Z}, \text{ which is determined by } \sigma_a(k) = a^k \sigma_a.$$

Also superscripts $+$ or $-$ will denote plus or minus parts.

Now we may state,

Iwasawa's Theorem (2.2).

$$(V_\infty/\mathscr{C}_\infty)^+ \cong A^+/(\mathscr{S}^*(-1))^+.$$

(See [I1 Proposition 3] or [C3 Theorem 7].)

We can rewrite the left hand side of the formula in Theorem B as

$$g(\mathfrak{p}_n, \psi)^{\omega_{a,b,c}-(1+\sigma_{-1})} \tag{2.3}$$

where $\omega_{a,b,c} = \sigma_{-a} + \sigma_{-b} + \sigma_{-c}$.

III. Ihara's series and the Hilbert norm residue symbol

Let $(\ ,\ )_{l^m}\colon \boldsymbol{Q}_l(\mu_{l^m})^* \times \boldsymbol{Q}_l(\mu_{l^m})^* \to \mu_{l^m}$ denote the Hilbert norm residue symbol defined by the formula

$$(a, b)_{l^m} = \sigma(\alpha)/\alpha$$

where $\sigma \in (G_{\boldsymbol{Q}_l(\mu_{l^m})})^{ab}$ is the image of b under the Artin map and α is any l^m-th root of a. (This is the same symbol as that discussed in [C2] and [CF] but the inverse of the symbol discussed in [I2] (note, however that formula (**) on page 353 of [CF] is the inverse of the truth).)

Theorem (3.1). *Suppose* $\sigma \in G_{\boldsymbol{Q}(\mu_{l^m})}$, $a+b+c=0$, $(abc, l)=1$, $\omega = \omega_{a,b,c}$ *and* $\varepsilon = (\varepsilon_n) \in (V_\infty)^+$. *Then*

$$(F_\sigma(\zeta_m^a, \zeta_m^b, \zeta_m^c), \varepsilon_m)_{l^m} = (\varepsilon_m^{(\omega\theta)^*(-1)})^{(\sigma-1)/l^m}. \tag{3.2}$$

The proof was inspired by the last argument of [G].

Proof. First, by the Tchebotarev Density Theorem, it suffices to prove the theorem when $\sigma=\mathrm{Frob}_{\mathfrak{p}}$ for some prime $\mathfrak{p}$ of $\boldsymbol{Q}(\mu_{l^m})$. For the moment we may let ω be any element in $I\cap \boldsymbol{Z}[[G]]$. Let d and k be integers such that $(d, l)=1$ and $\mathfrak{p}^{dl^k}=(\alpha)$ for some $\alpha \in \boldsymbol{Q}(\mu_{l^m})$. Second, let $d_n=\varepsilon_n^{(\omega\theta)^*(-1)}$. Then, by Iwasawa's Theorem, $(d_n)\in \mathscr{C}_\infty$. Hence, we can find an element $(c_n)\in \varprojlim \mathscr{C}_n$ such that c_{m+k} differs from d_{m+k} by an l^{m+k}-th power. In particular, the right hand side of (3.2) equals

$$c_m^{(\sigma-1)/l^m}=\left(\frac{c_m}{\mathfrak{p}}\right)_{l^m}$$

which is a global formula. Then by formal properties of the power and norm residue symbols, together with Artin reciprocity (See [CF] Exc. 1 & 2), after passing to the field $\boldsymbol{Q}(\mu_{l^{m+k}})$, the above equals:

$$\begin{aligned}\left(\frac{c_{m+k}}{(\alpha)}\right)_{l^{m+k}}^{1/d} &=(\alpha, c_{m+k})_{l^{m+k}}^{1/d}\\ &=(\alpha, \varepsilon_{m+k}{}^{(\omega\theta)^*(-1)})_{l^{m+k}}^{1/d}=(\alpha^{\omega\theta}, \varepsilon_{m+k})_{l^{m+k}}^{1/d}\\ &=(g(\mathfrak{p}, \psi)^{dl^k\omega}a\rho, \varepsilon_{m+k})_{l^{m+k}}^{1/d}\end{aligned}$$

where $a=N\mathfrak{p}^{-dl^k/2}\in \boldsymbol{Z}_l^*$ and ρ is a root of unity by Stickelberger's theorem. Since $\varepsilon\in V_\infty^+$, this equals, finally,

$$(g(\mathfrak{p}, \psi)^\omega, \varepsilon_m)_{l^m},$$

and when $\omega=\sigma_{-a}+\sigma_{-b}+\sigma_{-c}-(1+\sigma_{-1})$, this is the left hand side of (3.2) by (2.3). □

Corollary (3.3).

$$\boldsymbol{Q}(\cup J_n[l^\infty])=\boldsymbol{Q}(\mu_\infty, \cup \mathscr{C}_n^{1/l^\infty}).$$

Sketch of proof. Use Iwasawa's Theorem, the definition of Ihara's series and the non-degeneracy of the Hilbert Symbol. I.e., Iwasawa's Theorem tells you that you get all real circular units on the right hand side of the formula in the theorem and Ihara's definition of F_σ tells you that the left hand side governs all torsion points of l-power order on the Jacobians of Fermat curves of l-power degree. □

We will now deduce Ihara's conjecture. We will need to use the explicit reciprocity law to get a formula for the coefficients of F_σ from Theorem 3.1.

IV. Proof of Ihara's conjecture

Our notation will be as above and as in [C2]. In particular, we make A act on $\boldsymbol{Z}_l[[T-1]]$ and also on $\boldsymbol{Z}_l[[T-1]]^0$ by setting $T^\sigma = T^{\chi(\sigma)}$ for $\sigma \in G$, and extending by linearity and continuity. We set

$$\omega_n = \sum_{l^n} \sigma_a \in A$$

$$\Lambda f = \operatorname{Log} f(T) - \frac{\operatorname{Log} f(T^l)}{l} \in \boldsymbol{Z}_l[[T-1]]$$

for $f \in \boldsymbol{Z}_l[[T-1]]^*$. We let $\mathscr{S}$ and $\mathscr{N}$ denote the trace and norm operators as in [C2] and $\mathscr{V} = \{g \in \boldsymbol{Z}_l[[T-1]] : \mathscr{S}g = 0\}$. We set

$$\int_n g = l^{-n} \sum_{\zeta \in \mu_{l^n}} g(\zeta) = l^{-n} \mathscr{S}^n(g)(1).$$

Let $D = Td/dT$. We have the following formulas and congruences for this integral (see [C2]). Let $h \in \boldsymbol{Z}_l[[T-1]]$.

(4.1)
$$D^{(k)} \omega h = \omega(k) D^{(k)} h$$

(4.2)
$$\int_n h = l^{-n} \mathscr{S}^n h \Big|_1$$

(4.3)
$$\int_n Dh = 0 \bmod l^n$$

If f lies in $\mathscr{V}$, and $k \geq 0$ lies in $\boldsymbol{Z}$ then

(4.4)
$$\int_n f(T) \cdot h(T^l) = 0$$

and

(4.5)
$$\int_n f \cdot h \equiv (-1)^k \int_n D^{-k} f \cdot D^k h \bmod l^n$$

where $D^{-k}h$ is the unique element in $\mathscr{V}$ satisfying $D^k(D^{-k}h) = h$. (This element exists by the corollary to Theorem 3 of [C3].) These facts follow easily from [C2] (1)–(8) ((4.5) follows from (4.3) by integration by parts).

Lemma (4.6). *Suppose f and $g \in \mathscr{V}$. Then*

$$\int_n \omega_n(k) f \cdot g \equiv (-1)^k D^{-k} f(1) \cdot D^k g(1) \bmod l^n.$$

Proof. This will follow by (4.1) and (4.5) from

$$\int_n \omega_n f\cdot g\equiv f(1)\cdot g(1),$$

which we will now prove. Set

$$h_n(T)=\sum_{a=1}^{l^n} f(T^a).$$

Then

$$\omega_n f(T)=h_n(T)-h_{n-1}(T^l)$$

and if $0\leq m\leq n$ and ζ generates μ_{l^m} then

$$h_n(\zeta)=l^{n-m}\sum_{\varepsilon\in\mu_{l^m}} f(\varepsilon)=l^{n-m}(\mathscr{S}^m f)(1)$$

which equals zero if $m>0$ as $f\in\mathscr{V}$ and equals $l^n f(1)$ if $m=0$.

Now

$$\begin{aligned}\int_n \omega_n f\cdot g&=\int_n h_n\cdot g \qquad \text{(by 4.4)}\\ &=l^{-n}\sum_{\zeta\in\mu_{l^n}} h_n(\zeta)g(\zeta)=f(1)g(1)\end{aligned}$$

as required. □

We let $\mathscr{M}$ denote the group of fixed points, f, of $\mathscr{N}$ such that $f(1)\equiv 1 \bmod l$.

Lemma (4.7). *There exists a unique $f_0\in\mathscr{M}^+$ such that*

$$\Lambda f_0=\frac{T+T^{-1}}{2}.$$

Proof. This follows from Theorem 4 of [C3].

We will now recall the special cases needed below of the explicit formulas for the Hilbert norm residue symbol given in [C2]. Suppose $f(T)\in 1+(T-1)Z_l[[T-1]]$ and $g(T)\in Z_l((T-1))^*$ satisfies

$$N_{n,k}(g(\zeta_n))=g(\zeta_k)$$

for $1\leq k\leq n$. Then by Theorem 1 of [C2]

$$(f(\zeta_n),\, g(\zeta_n))_{l^n}=\zeta^{\langle f,g\rangle_n+\int_n \Lambda f\cdot Dg/g} \tag{4.7.1}$$

where $\langle f, g\rangle_n$ is an error term which vanishes when $Df(1)=0$ or when $N_n(g(\zeta_n))\in(l)\subseteq Q_l^*$. When g is a fixed point of the norm operator (which means that $(g(\zeta_m))$ is a coherent sequence under the norm) and $\alpha \in Z_l[\mu_{l^n}]^*$ then the above formula implies Iwasawa's formula, [I2]

$$(4.7.2) \qquad (\alpha, g(\zeta_n))_{l^n} = \zeta_n^{l^{-n}T_n(\mathrm{Log}(\alpha)\cdot(Dg/g)(\zeta_n))}$$

(see Corollary 15 of [C2]).

Proposition (4.8). *Suppose $g \in \mathscr{M}$ and*

$$g(T) = \exp\left(\sum_{m=1}^{\infty} b_m \frac{W^m}{m!}\right)$$

where $W = \mathrm{Log}(T)$. Then for m odd

$$(4.9) \qquad (f_0(\zeta_n)^{\omega_n(m-1)}, g(\zeta_n))_{l^n} = \zeta_n^{b_n(1-l^{m-1})}.$$

Proof. By (4.7.1), the left hand side of (4.9) equals ζ_n raised to the exponent

$$\int_n \omega_n(m-1)\Lambda f_0 \cdot D\,\mathrm{Log}\, g = \int_n \omega_n(m-1)\Lambda f_0 \cdot D\Lambda g$$

by (4.4) since $\Lambda f_0 \in \mathscr{V}$. But by Lemma 4.6, this equals, modulo l^n,

$$(-1)^{m-1} D^{-(m-1)}\left(\frac{T+T^{-1}}{2}\right)(1) \cdot D^m \Lambda g(1)$$

which equals 0 when m is even and

$$D^m \Lambda g(1) = b_m(1 - l^{m-1})$$

when m is odd. □

Proposition (4.10). *Suppose $\omega \in I$, then for m odd*

$$(f_0(\zeta_n)^{\omega_n(m-1)})^{(\omega\theta)^*(-1)} \equiv (c_{n,m})^{\chi^m(\omega)}$$

modulo l^n-th powers.

Proof.

$$\begin{aligned} &D\Lambda((f_0(T)^{\omega_n(m-1)})^{(\omega\theta)^*(-1)}) \\ &= (\omega\theta)^* \omega_n(m)\left(\frac{T-T^{-1}}{2}\right) = \omega_n(m)\omega^*\left(\frac{T}{T-1} - \frac{T^l}{T^l-1}\right) \\ &= D\Lambda(T^{-1/2} - T^{1/2})^{(\omega_n(m)\omega^*)(-1)} \end{aligned}$$

using Proposition 5 of [C3]. Now $\mathscr{N}(T^{-1/2} - T^{1/2}) = (T^{-1/2} - T^{1/2})$ and

$(T^{-1/2}-T^{1/2})^{\sigma-1}=-(T^{-1/2}-T^{1/2})$. It follows easily from this that $(T^{-1/2}-T^{1/2})^{\omega^*(-1)}$ lies in $\mathcal{M}^+$. Since $(f_0(T)^{\omega_n(m-1)})^{(\omega\theta)^*(-1)}$ also lies in $\mathcal{M}^+$, Theorem 4 of [C3] implies

$$(f_0(T)^{\omega_n(m-1)})^{(\omega\theta)^*(-1)}=\varepsilon(T^{-1/2}-T^{1/2})^{(\omega_n(m)\omega^*)(-1)}$$

for some $(l-1)$-st root of unity ε. Now,

$$\omega_n(m)\omega^*\equiv\chi^m(\omega)\omega_n(m) \qquad \bmod l^n$$

which gives us what we want. □

Now finally we can finish the proof of Ihara's conjecture. Let $a+b+c=0$, $(abc, l)=1$. First, by Theorem 3.1, Proposition 4.10 and the fact that for m odd $\chi^m(\omega_{-a,-b,-c})=-(a^m+b^m+c^m)$

$$(F_\sigma(\zeta_n^a, \zeta_n^b, \zeta_n^c), f_0(\zeta_n)^{\omega_n(m-1)})_{l^n}=(c_{n,m}^{(1-\sigma)/l^n})^{a^m+b^m+c^m}.$$

On the other hand,

$$F_\sigma(T^a, T^b, T^c)=\exp\left(\sum_{\substack{m\geq 3\\ m\text{ odd}}} b_m(\sigma)(a^m+b^m+c^m)\frac{W^m}{m!}\right)$$

and it follows from Anderson's theory of the hyperadelic gamma function (Corollary 5.5 below) that $F_\sigma(T^a, T^b, T^c)\in\mathcal{M}$ so by Proposition 4.8, and the skew symmetry of the Hilbert norm residue symbol,

$$(F_\sigma(\zeta_n^a, \zeta_n^b, \zeta_n^c), f_0(\zeta_n)^{\omega_n(m-1)})_{l^n}=\zeta_n^{-b_m(\sigma)(1-l^{m-1})(a^m+b^m+c^m)}.$$

Ihara's conjecture would follow immediately if we could cancel the exponents $a^m+b^m+c^m$. We can't quite since they may have positive valuation at l (we may choose a, b and c so that these exponents are not zero). However, by allowing n to increase and using the easy fact that $c_{n,m}/c_{n',m}$ is an l^n-th power for $n'\geq n$, we can ultimately cancel these exponents. □

V. Anderson's "Gamma" series

We now remove the restriction $l\neq 2$. We will discuss Anderson's theory of the hyperadelic gamma function which is developed in [A].

Notation.

$\bar{Q}=$: the algebraic closure of Q in the complex numbers C.

$W=$: the Witt vectors of $\bar{F}_l$.

$\Phi=$: the Frobenius automorphism of W.

$\Omega =:$ an element of W such that $\Omega^{\Phi}=\Omega+1$.

$K=:$ the fraction field of W.

$\bar{K}=:$ an algebraic closure of K.

$\boldsymbol{e}(x)=:$ $\exp(2\pi i x)$ $(x \in \boldsymbol{Q})$.

Definition (5.1). For each $\sigma \in G(\boldsymbol{Q})$, let $e(\sigma) \in \boldsymbol{Z}_l$ be defined by the system of congruences

$$(l^{1/l^n})^{\sigma-1}=\zeta_n^{e(\sigma)} \qquad (n \in \boldsymbol{Z}_{>0})$$

where l^{1/l^n} is the *positive* $(l^n)^{\text{th}}$ root of l.

In [A], § 7, (see 7.5.1) a series $G_\sigma(T) \in W[[T-1]]$ is constructed which satisfies the following properties (see § 8 of [A]):

Formulary (5.2).

(I) $\qquad G_\sigma(T) \in 1-e(\sigma)\Omega(T-1)+(T-1)^2 W[[T-1]]$ $(\sigma \in G_{\boldsymbol{Q}})$.

(II) $\qquad G_\sigma^{\omega}(T) \in 1+(T-1)^2 \boldsymbol{Z}_l[[T-1]]$ $(\omega \in I)$.

(III) $\qquad G_\sigma(T)G_\tau(T^{\chi(\sigma)})=G_{\sigma\tau}(T)$ $(\sigma, \tau \in G_{\boldsymbol{Q}})$.

(IV) $\qquad G_\rho(T)=1$ where ρ is complex conjugation.

(V) $(s\mapsto 1-s)$ $\quad G_\sigma(T)G_\sigma(T^{-1})=\chi(\sigma)S_\sigma(T)$ $(\sigma \in G_{\boldsymbol{Q}})$

where

$$S_\sigma(T)=:\ \frac{T^{1/2}-T^{-1/2}}{T^{\chi(\sigma)/2}-T^{-\chi(\sigma)/2}}$$

$$=(T-1)T^{(\chi(\sigma)-1)/2}(T^{\chi(\sigma)}-1)^{-1} \in \boldsymbol{Z}_l[[T-1]]^*.$$

(VI) $\qquad G_\sigma^{\Phi}(T)=T^{-e(\sigma)}G_\sigma(T)$

where G_σ^{Φ} is the power series obtained from $G_\sigma(T)$ by applying Φ to all the Taylor coefficients.

(VII) (Gauss multiplication)

$$\prod_{\eta^l=\lambda} G_\sigma(\eta)=G_\sigma^{\Phi}(\lambda)\prod_{\zeta^l=1} G_\sigma(\zeta) \qquad (\sigma \in G_{\boldsymbol{Q}},\ \lambda \in \mu_{l^\infty}(\bar{K}_l)).$$

It follows from (I), (V) and (VII) that

(VIII) $\qquad \mathcal{N}G_\sigma=G_\sigma^{\Phi} \qquad$ for $\sigma \in G_{\boldsymbol{Q}(\mu_{l^\infty})}$

(even when $l=2$, as $e(\sigma)\equiv 0$ (2) if $\sigma \in G_{\boldsymbol{Q}(\mu_{2^\infty})}$).

Moreover, these series are related to Gauss sums in the way Ihara's series are related to Jacobi-sums. I will just state the special case I will need in the following. Fix an embedding τ: $\bar{\boldsymbol{Q}}\to\bar{K}_l$. Set $\zeta_n=\tau(\boldsymbol{e}(-l^{-n}))$.

Theorem (5.3). *For each rational prime p distinct from l there exists a non-trivial character* $\psi_p\colon \boldsymbol{F}_p \to \bar{\boldsymbol{Q}}$ *such that for all* $n \geq 0$ *and all primes* $\mathfrak{p}$ *of* $\boldsymbol{Q}(\zeta_n)$ *of residue characteristic p*

$$G_\sigma(\zeta_n) = \tau(g(\mathfrak{p}, \psi_p))$$

where σ *is any* $\mathfrak{p}$*-Frobenius element.*

Remark. Using the cocycle condition 5.2(III) one can factor the left hand side of the above formula and make this theorem look more like Theorem B.

These series are closely related to Ihara's series above, for example,

Theorem (5.4). *Suppose* $\sigma \in G_{\boldsymbol{Q}(\mu_{l^\infty})}$, *then*

$$G_\sigma(R)G_\sigma(S)G_\sigma(T) = F_\sigma(R, S, T), \qquad (RST = 1).$$

It follows from this and (5.2)VIII that

Corollary (5.5). *Suppose* $\sigma \in G_{\boldsymbol{Q}(\mu_{l^\infty})}$, $a+b+c=0$ *and* $(abc, l)=1$, *then*

$$\prod_{\zeta^l=1} F_\sigma(\zeta^a R, \zeta^b S, \zeta^c T) = F_\sigma(R^l, S^l, T^l)$$

and in particular, $F_\sigma(T^a, T^b, T^c) \in \mathcal{M}$.

Remark. The formula relating G_σ to F_σ looks much more like the classical formula relating the gamma function to the beta function if one improves the definitions in the way indicated in § 1. Also I should point out that the foregoing is only the l-adic case of Anderson's "hyperadelic gamma function".

When σ does not lie in $G_{\boldsymbol{Q}(\mu_{l^\infty})}$ the relationship is much more complicated (see § 13 of [A]).

One can show that

$$(5.6) \qquad G_\sigma(T) = \exp\left(\sum_{\substack{m=1 \\ m \text{ odd}}}^{\infty} b_m(\sigma)\frac{W^m}{m!}\right)$$

where W and $b_m(\sigma)$ for $m \geq 3$ are defined as in § 1 and $b_1(\sigma)$ is such that

$$(5.7) \qquad (l^{1/l^n})^{\sigma-1} = e(1/l^n)^{b_1(\sigma)}.$$

VI. Local components of Jacobi sum Hecke characters

This section will be a preview of joint work with Greg Anderson. Another application of the Anderson-Ihara Theory is a new proof of (at least the wild part of) the formula proven with McCallum [CM] for the local components of Jacobi sum Hecke characters coming from Fermat curves. This approach also provides the answers when the prime 2 is involved and should, in principle, allow one to compute the conductors of the most general Jacobi sum Hecke characters.

Let $\omega \in I \cap \boldsymbol{Z}[[G]]$. Fix n for now and set $K=\boldsymbol{Q}(\zeta_n)$. Then for each prime $\mathfrak{p}$ of K, not dividing l, the correspondence

$$\mathfrak{p} \longmapsto g(\mathfrak{p}, \psi)^{\omega}$$

gives rise, in the standard way, to a continuous Serre-Tate character $\rho_n\colon I_k \to I_k$, from the idèles of K into itself such that

$$(\rho_n(s))_v = g(\mathfrak{p}, \psi)^{\omega} \in K_v^*,$$
$$\rho_n(\alpha) = 1$$

where s is an idèle which is a local uniformizing parameter at $\mathfrak{p}$ in the $\mathfrak{p}$-th place and ones elsewhere, v is a place different from $\mathfrak{p}$ and $\alpha \in K^* \subseteq I_K$. Moreover, if λ is a prime of K and $b \in O_\lambda^* \subseteq I_K$, considered as an idèle in the natural way, then

$$(\rho_n(b))_\lambda b^{\omega\theta_n'} = \text{ a root of unity in } K_\lambda^*$$

($\omega\theta_n'$ is the infinity type). The determination of this root of unity is the determination of the local component of ρ_n at λ. It is trivial unless λ is the prime above l and so we will suppose this from now on.

When $\omega = \sigma_{-a} + \sigma_{-b} + \sigma_{-c} - (1 + \sigma_{-1})$, where $a+b+c=0$, $(abc, l)=1$, then $s \mapsto \rho_n(s) s^{\omega\theta_n'}$ is a Jacobi sum Hecke character attached to the Fermat curve of degree l^n mentioned above (but not all such characters are of this form because of the condition $(abc, l)=1$).

Proposition (6.–1). *Suppose $s \in I_K$. Let $\sigma \in G_{\boldsymbol{Q}}$ whose restriction to $(G_{\boldsymbol{Q}(\mu_{l^\infty})})^{ab}$ is the image of s under the Artin map. Then*

$$G_\sigma^\omega(\zeta_n) = \rho_n(s)_\lambda.$$

Proof. This follows from Theorem 5.3 and the Tchebotarev Density Theorem.

Corollary (6.0). *With notation as before, if $b=(b_m) \in U_\infty$, and we identify b with its image in $(G_{\boldsymbol{Q}(\mu_{l^\infty})})^{ab}$ under the Artin map, then $G_b^\omega(\zeta_m) = \rho_m(b_m)$ for all $m \geq 0$.*

Now by Theorem A of [C1], there exists an $f_b \in \boldsymbol{Z}_l[[T-1]]^*$ such that $f_b(\zeta_n) = b_n$. Therefore,

$$(G_b^{\omega}f_b^{\omega\theta})(\zeta_n)=\rho_n(b_n)_l b_n^{\omega\theta}=\text{an } l^n\text{-th root of unity},$$

for all n (since $b_n^{\omega_n}=1$).

Lemma (6.1). *Suppose $H(T)\in Z_l[[T-1]]^*$, is such that $H(\zeta_n)$ is an l-power root of unity for all n. Then*

$$H(T)=H(1)T^{(DH/H)(1)}$$

and $H(1)\in\mu_l(Q_l)$.

Proof. The series ΛH lies in $Z_l[[T-1]]$ and vanishes on ζ_n for all n. It follows that $\Lambda H=0$. The result now follows from Theorem 1 of [C3]. □

Applying this to $H=G_b^{\omega}f_b^{\omega\theta}$ and using 5.2(II), and the fact that $\omega\theta\in A^-$ we have

$$\rho_n(b_n)_l b_n^{\omega\theta}=\zeta_n^k$$

where

$$k=(Df_b^{\omega\theta}/f_b^{\omega\theta})(1)=\chi(\omega\theta)\cdot(Df_b/f_b)(1).$$

Now one can evaluate this in terms of ω.

Lemma (6.2) (Iwasawa [13]).

$$\chi((1-a^{-1}\sigma_a)\theta)=\frac{l-1}{l}\cdot\operatorname{Log} a.$$

Proof.

$$\chi((1-a^{-1}\sigma_a)\theta)=\lim_{n\to\infty}\sum_b{}_n\,(ab)^{-1}\left[\frac{ab}{l^n}\right]+\frac{(1-a^{-1})b}{2}$$

On the other hand

$$ab=b'\left(1+b'^{-1}\left[\frac{ab}{l^n}\right]^{l^n}\right)$$

where

$$b'=l^n\left\langle\frac{ab}{l^n}\right\rangle.$$

Taking logarithms we have

$$\mathrm{Log}\,(a)+\mathrm{Log}\,(b)=\mathrm{Log}\,(b')+\mathrm{Log}\left(1+b'^{-1}\left[\frac{ab}{l^n}\right]^{l^n}\right)$$
$$\equiv \mathrm{Log}\,(b')+(ab)^{-1}\left[\frac{ab}{l^n}\right] \bmod l^{2n}/2.$$

Now summing over $0<b<l^n$, $(b, l)=1$, we deduce that

$$\frac{l-1}{l}\cdot \mathrm{Log}\,(a)\equiv \textstyle\sum_n (ab)^{-1}\left[\frac{ab}{l^n}\right] \bmod l^n/2.$$

From this the lemma follows easily. □

Suppose now that $a_1+a_2+\cdots+a_n=0$, $(a_1a_2\cdots a_n, l)=1$ and $\omega=\sigma_{-a_1}+\sigma_{-a_2}+\cdots+\sigma_{-a_n}$ then as

$$\omega=\textstyle\sum a_i(1-(-a_i)^{-1}\sigma_{-a_i})$$

the above lemma implies

$$k=\frac{l-1}{l}\cdot \mathrm{Log}\,(a_1^{a_1}a_2^{a_2}\cdots a_n^{a_n})\cdot(Df_b/f_b)(1). \tag{6.3}$$

But now ζ_n^k can be interpreted by means of Iwasawa's explicit reciprocity law:

Theorem (6.4). *Let $\beta \in U_n^0$. Then, with notation as above, if l is odd or $l=2$ and $N_n\beta\equiv 1 \bmod 2^{n+2}$*

$$\rho_n(\beta)_\lambda\beta^{\omega\theta'_n}=(a_1^{a_1}a_2^{a_2}\cdots a_n^{a_n}, \beta)_{l^n}. \tag{6.5}$$

Proof. First, it follows from (6.3) and Iwasawa's explicit reciprocity law, (4.7.2) above, that this is true if $N_n\beta=1$ since then $\beta=b_n$ for some sequence $(b_n)\in U_\infty^0$. Set $\alpha(\beta)=\rho_n(\beta)_\lambda\beta^{\omega\theta'_n}$. Then if $\sigma\in G$, it is easy to see that $\alpha(\beta^\sigma)=\alpha(\beta)^\sigma$. So if $\beta\in 1+l\boldsymbol{Z}_l$, we must have $\alpha(\beta)=1$ if l is odd and $\alpha(\beta)=\pm 1$ if $l=2$. Suppose for the moment that l is odd. Then if $\beta\in 1+l\boldsymbol{Z}_l$ then the right hand side of (6.5) is 1 also and as the elements of norm 1 and the elements in $\boldsymbol{Z}_l^*$ generate U_n^0, this establishes the theorem in this case. Similarly, when $l=2$, both sides of (6.5) are one when $\beta\in 1+8\boldsymbol{Z}_2$ and $1+8\boldsymbol{Z}_2$ together with the elements of norm 1 to $\boldsymbol{Q}_2$ generate the group of units whose norm is congruent to 1 modulo 2^{n+2}. □

Remarks. (1) When $l=2$, the subgroup of U_n^0 consisting of units whose norm is congruent to 1 modulo 2^{n+2} is of index 4.

(2) To deduce the corresponding result for the remaining Jacobi sum Hecke characters attached to Fermat curves from this one, one must

make use of the Hasse-Davenport relation for Gauss sums, which translates, in this context, into the Gauss multiplication formula for Anderson's gamma function. More precisely, using the Hasse-Davenport relation as in [CM] § 7, one can show that when l is odd the above Hecke-characters and the Hecke-character $\mathfrak{p} \mapsto \left(\frac{l}{\mathfrak{p}}\right)$ generate a group of Hecke characters containing all those attached to Fermat curves and when $l=2$ these together with one more generate such a group.

(3) This result, when l is odd, is a special case of a more general result obtained previously with McCallum, by a totally different method. In fact, one might say the two approaches come from different sides of the explicit reciprocity law. Together they give a new proof of the special case of the explicit reciprocity law just used.

VII. G_σ for σ in inertia and Vandiver's conjecture

In this section, we will give a formula without proof for G_σ when the restriction of σ to $(G_{Q(\mu_{l\infty})})^{ab}$ lies in the inertia group above l and explain how one can re-express Vandiver's conjecture in terms of Anderson's gamma function.

Let $\mathscr{V}$ and $\mathscr{M}$ be as in § 4. Then $\mathscr{M} \cong U_\infty$, via the map $f \mapsto (f(\zeta_n))$. By Theorem 3 of [C3] $\mathscr{V}$ is a principal A-module and the map $f \mapsto \Lambda f$ takes $\mathscr{M}$ onto $I\mathscr{V}$ (the kernel is generated by T). This means we can make sense of $e\Lambda f$ for f in $\mathscr{M}$. Indeed, write $\Lambda f = \omega g$ for $\omega \in I$ and $g \in \mathscr{V}$ and set $\theta \Lambda f = (\omega\theta) g$. This is well defined. We extend Λ to $W[[T-1]]^*$ by setting

$$\Lambda f(T) = \operatorname{Log} f(T) - \frac{\operatorname{Log} f^{\Phi}(T^l)}{l}$$

for $f \in W[[T-1]]^*$. Now let $\Omega \in W$ be as in § 5 (recall, $\Omega^{\Phi} = \Omega + 1$). Define

$$E: \mathscr{V} \longrightarrow W[[T-1]]^*$$

by

$$E(g) =: \exp\left(\frac{l}{l-1} \cdot g(1) + Dg(1) \cdot \gamma(T) + \sum_{n=0}^{\infty} \frac{g^*(T^{l^n})}{l^n}\right)$$

for $g \in \mathscr{V}$, where

$$\gamma(T) = \sum_{n=0}^{\infty} \left(\frac{T^{l^n}}{l^n} - \operatorname{Log}(T)\right) - \Omega \operatorname{Log}(T)$$

and

$$g^*(T)=g(T)-(g(1)+Dg(1)T).$$

Then an easy computation reveals

Lemma (7.1). $\Lambda(E(g))=g.$

For $f \in \mathcal{M}$ we set

$$f^\theta=E(\theta\Lambda f).$$

Now suppose $\sigma \in G_{Q(\mu_{l\infty})}$ such that the restriction of σ to $(G_{Q(\mu_{l\infty})})^{ab}$ lies in the wild part of the inertia group above l. Then σ corresponds to an element of U_∞ which in turn corresponds to an element f_σ of $\mathcal{M}$ as explained above. We have

Theorem (7.2). *For all $\sigma \in G_{Q(\mu_{l\infty})}$ whose image in $(G_{Q(\mu_{l\infty})})^{ab}$ lies in inertia*

$$G_\sigma=f_\sigma^\theta.$$

Sketch of proof for l odd. Let $B_\sigma(R, S, T)=f_\sigma^\theta(R)f_\sigma^\theta(S)f_\sigma^\theta(T)$, $(RST=1)$. Then it is easy to see that $B_\sigma(R, S, T) \in \Lambda$, that $B_\sigma(R^{-1}, S^{-1}, T^{-1})=B_\sigma(R\ S, T)^{-1}$ and if $a+b+c=0$, $(abc, l)=1$ that

$$B_\sigma(T^a, T^b, T^c)=f_\sigma^{\omega_{a,b,c}\theta}.$$

From this and Theorem 3.1, it follows that $B_\sigma(R\ S, T)=F_\sigma(R, S, T)$. The result eventually follows from this, Theorem 5.4 and (5.2)I. □

It follows from (5.2)V and (5.2)VII that $\Lambda G_\sigma \in \mathcal{V}^-$.

Theorem (7.3). *Suppose l is odd. Then the map Γ: $G_{Q(\mu_{l\infty})}\to\mathcal{V}^-$, $\sigma\mapsto\Lambda G_\sigma$, is surjective iff Vandiver's conjecture is true.*

Proof. Since $\mathcal{V}$ is a principal Λ module (4.1) implies Γ is surjective iff for each odd integer $0<i<(l-1)$ there exists a $\sigma \in G_{Q(\mu_{l\infty})}$ such that $D^i\Lambda G_\sigma(1)$ is an l-adic unit. First recall, by (5.6) and (5.7),

$$(l^{1/l^n})^{\sigma-1}=e(1/l^n)^{b_1(\sigma)}.$$

Hence, since l has no l-th root in $Q(\mu_{l\infty})$ there exists a σ such that $D\Lambda G_\sigma(1)$ is a unit. Next suppose i is odd and greater than 1. Then, it follows from Theorem C and (5.6) that

$$(c_{1,i})^{\sigma-1}=e(l^{-1})^{D^i\Lambda G_\sigma(1)}.$$

As Vandiver's conjecture is equivalent to the elements $c_{1,i}$ not being l-th powers in $Q(\mu_{l^\infty})$ for odd i, $1<i<l-1$, the theorem follows. □

Bibliography

[A] Anderson, G., The Hyperadelic Gamma Function, to appear.

[CF] Cassels, Frohlich, Algebraic Number Theory, Academic Press, London (1969).

[C1] Coleman, R., Division Values in Local Fields, Invent. Math., **53** (1979), 91–116.

[C2] ——, The Dilogarithm and the Norm Residue Symbol, Bull. Soc. math. France, **109** (1981), 373–402.

[C3] ——, Local Units Modulo Circular Units, Proc. Amer. Math. Soc., **89** No. 1 (1983), 1–7.

[CM] ——, W. McCallum, Stable Reduction of Fermat Curves and Jacobi Sum Hecke Characters, to appear in J. Reine Angew. Math.

[G] Greenberg, R., On the Jacobian Variety of Some Algebraic Curves, Compositio Math., **42** (1981), 345–359.

[I] Ihara, Y., Profinite Braid groups, Galois representations and complex multiplications, Ann. of Math., **123** (1986), 43–106.

[IKY] Ihara, Y., M. Kaneko and A. Yukinari, On Some Properties of the Universal Power Series for Jacobi Sums, Adv. Studies in Pure Math., **12** (1987), 65–86.

[I1] Iwasawa, K., On Some Modules in the Theory of Cyclotomic Fields, J. Math. Soc. Japan, **16** (1964), 42–82.

[I2] ——, On explicit formulas for the norm residue symbol, J. Math. Soc. Japan, **20** (1968), 151–164.

[I3] ——, Lectures on p-adic L-Functions, Princeton Univ. Press, (1972).

[L] Lang, S., Cyclotomic Fields, Springer-Verlag, (1978).

Errata to "Local Units Modulo Circular Units"

In the fifth displayed equation on page 3, $[a](T)$ should be replaced by $T/[a](T)$.
In the seventh displayed equation page 3, σ_a should be replaced by $\sigma_a{}^{-1}$.
In the sixth line on page 5, A_k should be replaced by A_∞.
In the eleventh line on page 5, Corollary 3.6 should be replaced by Corollary 13.6.
In the fourth displayed equation on page 6, $x \in L$ should be replaced by $x \in \boldsymbol{Z}$.
In Theorem 10, p^{n+1} should be replaced by p^n.

Department of Mathematics
University of California
Berkeley, CA 94720
U.S.A.