W. SINNOTT

On a theorem of L. Washington

Astérisque, tome 147-148 (1987), p. 209-224
<http://www.numdam.org/item?id=AST_1987__147-148__209_0>

Société Mathématique de France
Astérisque 147-148 (1987), p.209-224.

ON A THEOREM OF L. WASHINGTON

BY

W. SINNOTT

Introduction.

Let F be a finite abelian extension of the rational numbers $\mathbb{Q}$, p a prime number, and $\mathbb{Q}_\infty$ the $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Let $F_\infty = F\mathbb{Q}_\infty$, and for each integer $n \geq 0$, let h_n denote the class number of the unique extension F_n of F in F_∞ of degree p^n over F. Then a theorem of L. Washington [3] states that, for any prime number $\ell \neq p$, the power of ℓ that divides h_n is constant for n sufficiently large.

To prove his theorem, Washington reduces it to an assertion (recalled in §4, below) about the ℓ-adic valuations of the values of Dirichlet's L-functions at $s = 0$. We give here a proof of this assertion, somewhat different from Washington's, based on the fact that these L-function values are "generated by rational functions" ; more precisely, we prove in §3 a general result applicable to any rational function measure, and apply to it the proof of Washington's theorem in §4.

§1. Preliminaries on Measure.

1.1. Notations: We fix two distinct prime numbers ℓ and p. $\mathbb{Z}_p$ denotes the ring of p-adic integers, $\mathbb{F}_\ell$ the prime field with ℓ elements, $\overline{\mathbb{F}}_\ell$ its algebraic closure, and μ_{p^∞} the group of all p-power roots of unity in $\overline{\mathbb{F}}_\ell$.

We recall that the group $\mathbb{Z}_p^\times$ of units in $\mathbb{Z}_p$ is the internal direct product of its torsion subgroup V and the subgroup $U = 1+2p\mathbb{Z}_p$.

1.2. Measures on $\mathbb{Z}_p$ with values in $\overline{\mathbb{F}}_\ell$: By a measure on $\mathbb{Z}_p$ with values in $\overline{\mathbb{F}}_\ell$ we mean a finitely additive $\overline{\mathbb{F}}_\ell$ -valued set function on the collection of compact open subsets of $\mathbb{Z}_p$. If α is a measure, and $\phi : \mathbb{Z}_p \to \overline{\mathbb{F}}_\ell$ is a locally constant function, say constant on the cosets of $p^n \mathbb{Z}_p$ in $\mathbb{Z}_p$, then we define the integral

$$(1.3) \qquad \int_{\mathbb{Z}_p} \phi(x)d\alpha(x) = \sum_{a \bmod p^n} \phi(a)\alpha(a+p^n \mathbb{Z}_p) .$$

1.4. Restriction and change of variable: If α is a measure and $X \subseteq \mathbb{Z}_p$ is compact and open, we denote by $\alpha|_X$ the measure obtained by restricting α to X and extending by 0 . We also define

$$(1.5) \qquad \int_X \phi(x)d\alpha(x) = \int_{\mathbb{Z}_p} \phi(x)d\alpha|_X (x) ,$$

for any locally constant function $\phi: \mathbb{Z}_p \to \overline{\mathbb{F}}_\ell$.

If $c \in \mathbb{Z}_p^\times$, we let $\alpha \circ c$ denote the measure defined by $\alpha \circ c\,(X) = \alpha(cX)$ for all compact open subsets $X \subseteq \mathbb{Z}_p$. In place of $d\alpha\circ c(x)$ we write $d\alpha(cx)$, so that we have the "change of variable" formula

$$(1.6) \qquad \int_{\mathbb{Z}_p} \phi(cx)d\alpha(cx) = \int_{\mathbb{Z}_p} \phi(x)d\alpha(x) .$$

We note that

$$(1.7) \qquad \alpha\circ c \Big|_X = \alpha \Big|_{cX} \circ c .$$

1.8. The Fourier Transform: We identify the continuous characters $\mathbb{Z}_p \to \overline{\mathbb{F}}_\ell^\times$ with the group $\mu_{p^\infty} \subseteq \overline{\mathbb{F}}_\ell$, an element $\zeta \in \mu_{p^\infty}$ corresponding to the character $x \mapsto \zeta^x$ $(x \in \mathbb{Z}_p)$. Let α be a measure ; the Fourier transform $\hat{\alpha}: \mu_{p^\infty} \to \overline{\mathbb{F}}_\ell$ of α is defined by

$$(1.9) \qquad \hat{\alpha}(\zeta) = \int_{\mathbb{Z}_p} \zeta^x \, d\alpha(x) .$$

By "Fourier inversion" we see that the Fourier transform gives an isomorphism between the ring (under convolution) of measures on $\mathbb{Z}_p$ with values in $\overline{\mathbb{F}}_\ell$ and the ring of functions on μ_{p^∞} with values in $\overline{\mathbb{F}}_\ell$.

It follows from (1.6) that, for any measure α,

$$\alpha\circ c\ (\zeta) = \hat{\alpha}\ (\zeta^{1/c}), \tag{1.10}$$

for $c \in \mathbb{Z}_p^\times$, $\zeta \in \mu_{p^\infty}$.

1.11. The Γ- Transform: Let Φ denote the group of continuous characters $U \to \overline{\mathbb{F}}_\ell^\times$, viewed always as characters of $\mathbb{Z}_p^\times$ trivial on V. Let α be a measure; the Γ - transform $\Gamma_\alpha : \Phi \to \overline{\mathbb{F}}_\ell$ of α is defined by

$$\Gamma_\alpha(\psi) = \int_{\mathbb{Z}_p^\times} \psi(x) d\alpha(x). \tag{1.12}$$

One relation between the two transforms is the following. Let $\psi \in \Phi$ and let $1 + p^n \mathbb{Z}_p$ be the kernel of ψ in U. View ψ as above as a character of $\mathbb{Z}_p^\times$ trivial on V, and extend ψ by 0 to all of $\mathbb{Z}_p$. Then we may write ψ as a linear combination of additive characters

$$\psi(x) = \frac{1}{p^n} \sum_{\zeta \in \mu_{p^n}} \tau(\psi,\zeta)\zeta^x, \tag{1.13}$$

with coefficients

$$\tau(\psi,\zeta) = \sum_{\substack{x \bmod p^n \\ x \not\equiv 0 \bmod p}} \psi(x)\zeta^{-x}; \tag{1.14}$$

therefore

$$\Gamma_\alpha(\psi) = \sum_{\zeta \in \mu_{p^n}} \tau(\psi,\zeta)\ \hat{\alpha}\ (\zeta). \tag{1.15}$$

When $n > 0$, $\tau\ (\psi,\zeta)$ is a primitive Gauss sum, and so vanishes unless ζ has order p^n. So for $n > 0$ the sum in (1.15) may be restricted to primitive p^n-the roots of unity ζ.

1.16. Rational Function Measures: We call a measure α a rational function measure if there is a rational function $R(Z) \in \overline{\mathbb{F}}_\ell(Z)$ such that

$$\hat{\alpha}(\zeta) = R(\zeta)$$

for almost all (i.e. all but finitely many) $\zeta \in \mu_{p^\infty}$.

If α is a rational function measure, then so is $\alpha|_X$ for any compact open subset $X \subseteq \mathbb{Z}_p$. In particular, if $X = \mathbb{Z}_p^\times$ and we put $\alpha^* = \alpha|_{\mathbb{Z}_p^\times}$, then we have

$$\hat{\alpha}^*(\zeta) = \hat{\alpha}(\zeta) - \frac{1}{p} \sum_{\varepsilon^p=1} \hat{\alpha}(\varepsilon\zeta) .$$

It follows that α is supported in $\mathbb{Z}_p^\times$ if and only if

(1.17) $$\sum_{\varepsilon^p=1} \hat{\alpha}(\varepsilon\zeta) = 0 , \quad \zeta \in \mu_{p^\infty} ;$$

this implies the identity

(1.18) $$\sum_{\varepsilon^p=1} R(\varepsilon Z) = 0 ,$$

where R(Z) is the rational function associated to α. (For details in a similar case, see [1], Lemma 1.1).

Finally, if k is the finite field generated over $\mathbb{F}_\ell$ by the coefficients of R(Z) and the values $\hat{\alpha}(\zeta)$ for which $\hat{\alpha}(\zeta) \neq R(\zeta)$, then α takes values in k.

§2. Power Functions on μ_{p^∞}.

2.1. Independence of Power Functions: Let z denote a "variable element" of μ_{p^∞}, so that we may define functions on μ_{p^∞} by means of expressions involving z. For any $a \in \mathbb{Z}_p$, we have the "a-th power map" z^a; it is the Fourier transform of the Dirac measure of mass 1 at a. We have:

Theorem 2.2: *Let* $b_1,\ldots,b_n$ *be elements of* $\overline{\mathbb{F}}_\ell$, *not all* 0, *and let* $a_1,\ldots,a_n$ *be distinct elements of* $\mathbb{Z}_p$. *Define* $f : \mu_{p^\infty} \longrightarrow \overline{\mathbb{F}}_\ell$ *by*

$$f(z) = \sum_{i=1}^{n} b_i z^{a_i} .$$

Then f *has only finitely many zeros in* μ_{p^∞}.

Proof: Let k be the field generated over the prime field $\mathbb{F}_\ell$ by $b_1,\ldots,b_n$ and the p-th roots of unity, and let p^{N_0} be the number of p-power roots of unity in k. Let N_1 be an integer large enough that $a_1,\ldots,a_n$ are distinct mod p^{N_1}. Suppose that $f(\zeta) = 0$, where ζ has order p^N and $N \geq N_0 + N_1$. Let Tr denote the trace map from $k(\zeta)$ to k. Then, for each $j = 1,\ldots n$,

$$0 = \mathrm{Tr}\,(\zeta^{-a_j} f(\zeta)) = [k(\zeta):k]b_j,$$

since if $i \neq j$, $\zeta^{a_i - a_j} \notin k$ and hence has trace 0. Since $[k(\zeta):k] = p^{N-N_0}$, it follows that $b_1=\ldots=b_n=0$, contrary to hypothesis. Thus all of the zeros of f lie in $\mu_{p^{N_0+N_1-1}}$, which completes the proof.

Let $\mathcal{F}$ denote the $\overline{\mathbb{F}}_\ell$-algebra of maps from μ_{p^∞} to $\overline{\mathbb{F}}_\ell$; and let $\mathcal{F}_0 = \mathcal{F}/N$, where N is the ideal of functions which vanish almost everywhere. The conclusion of the theorem states that $f(Z)$ is a unit in $\mathcal{F}_0$.

Corollary 2.4: *If $a_1,\dots,a_n$ are elements of $\mathbb{Z}_p$ linearly independent over $\mathbb{Z}$, then the functions $z^{a_1},\dots,z^{a_n}$ are algebraically independent over $\overline{\mathbb{F}}_\ell$ in $\mathcal{F}_0$. Let $X_1,\dots,X_n$ be independent indeterminates over $\overline{\mathbb{F}}_\ell$: then sending $X_i \to z^{a_i}$, $i = 1,\dots,n$, induces an inclusion*

$$\overline{\mathbb{F}}_\ell(X_1,\dots,X_n) \to \mathcal{F}_0 .$$

Proof: In any case there is a map from the polynomial ring $\overline{\mathbb{F}}_\ell[X_1,\dots,X_n]$ to $\mathcal{F}_0$, sending X_i to z^{a_i} for each i. A monomial $X_1^{k_1}\dots X_n^{k_n}$ is sent to the power map $z^{k_1a_1+\dots+k_na_n}$, so, since $a_1,\dots,a_n$ are linearly independent over $\mathbb{Z}$, distinct monomials are sent to distinct power maps. Hence if $F(X_1,\dots,X_n)$ is a non-zero polynomial in $\overline{\mathbb{F}}_\ell[X_1,\dots,X_n]$, $F(z^{a_1},\dots,z^{a_n})$ is a unit in $\mathcal{F}_0$, by Theorem 2.2; this proves the corollary.

§3. The Main Theorem.

3.1: We prove here a general result about Γ-transforms of rational functions; in the next section we apply this result to prove Washington theorem.

Theorem 3.2: *Let α be a rational function measure on $\mathbb{Z}_p$ with values in $\overline{\mathbb{F}}_\ell$, and let $R(Z) \in \overline{\mathbb{F}}_\ell(Z)$ be the associated rational function. Assume that α is supported on $\mathbb{Z}_p^\times$. If*

$$\Gamma_\alpha(\psi) = 0$$

for infinitely many $\psi \in \Phi$, then

$$R(Z) + R(Z^{-1}) = 0 .$$

Proof: Since $\mathbb{Z}_p^\times = V \times U$ (see (1.1)), we may write

$$\Gamma_\alpha(\psi) = \sum_{\eta \in V} \int_{\eta U} \psi(x)d\alpha(x) \; ;$$

then, making the change of variable $x \to \eta x$ in the integral, we have

$$(3.3) \qquad \Gamma_\alpha(\psi) = \sum_{\eta \in V} \int_U \psi(x)d\alpha(\eta x) = \int_U \psi(x)d\beta(x) \; ,$$

with

$$(3.4) \qquad \beta = \sum_{\eta \in V} \alpha \circ \eta \; .$$

By (1.16), α, and therefore also β, takes values in a finite subfield $k \subseteq \overline{\mathbb{F}}_\ell$. We may suppose that $\mu_p \subseteq k$ (resp. $\mu_4 \subseteq k$ if $p = 2$). Let p^{n_0} be the number of p-power roots of unity in k and let $k_n = k(\mu_{p^{n_0+n}})$ for $n \geq 0$. Note that if ζ is a p-power root of unity in k_n, then

$$(3.5) \qquad p^{-n}\mathrm{Tr}_{k_n/k}(\zeta) = \zeta \text{ if } \zeta \in \mu_{p^{n_0}} \; , \qquad = 0 \text{ if } \zeta \notin \mu_{p^{n_0}} \; .$$

Let $K = \bigcup_n k_n$. The action of Gal(K/k) on μ_{p^∞} gives a natural isomorphism $\mathrm{Gal}(K/k) \simeq 1 + p^{n_0}\mathbb{Z}_p$. For $t \in 1 + p^{n_0}\mathbb{Z}_p$, we let σ_t denote the corresponding automorphism of K/k, so that $\sigma_t(\zeta) = \zeta^t$ for $\zeta \in \mu_{p^\infty}$.

Lemma 3.6. Let $\psi \in \Phi$ and let p^m be the conductor of ψ (i.e. $1 + p^m\mathbb{Z}_p$ is the kernel of ψ in U). Assume that $\Gamma_\alpha(\psi) = 0$ and that $m \geq 2n_0$. Let $n = m - n_0$ and let $\zeta_\psi \in \mu_{p^\infty}$ satisfy $\zeta_\psi^{p^n} = \psi(1 + p^n)$ (then

ζ_ψ has order $p^{n+n_0} = p^m$). Finally, for each $y \in U$ let $\beta_y = \beta|_{y(1+p^{n_0}\mathbb{Z}_p)}$ (β_y depends only on y mod $p^{n_0}\mathbb{Z}_p$). Then for each $y \in U$, we have

$$\hat{\beta}_y(\zeta_\psi^{1/y}) = 0 .$$

Proof: Let $y \in U$. Multiply (3.3) by $\psi(y)^{-1}$ and take the trace from k_n to k: since $\Gamma_\alpha(\psi) = 0$, and since $\psi(x/y) \in \mu_{p^{n_0}}$ only if $x/y \in 1 + p^n\mathbb{Z}_p$, we obtain

$$0 = \int_{y(1+p^n\mathbb{Z}_p)} \psi(x/y)\,d\beta(x) , \tag{3.7}$$

using (3.5). Let $x \in y(1 + p^n\mathbb{Z}_p)$ and write $x = y(1 + p^n z)$.

Then

$$\psi(x/y) = \psi(1 + p^n z) = \psi(1 + p^n)^z = \zeta_\psi^{p^n z} = \zeta_\psi^{x/y-1} ;$$

The second equality requires the hypothesis $m \geq 2n_0$, i.e. $n \geq n_0$:

$$(1 + p^n)^z \equiv 1 + p^n z \mod p^{2n} ,$$

hence the congruence holds mod p^m, the conductor of ψ. Using (3.8) in (3.7), we find

$$\int_{y(1+p^n\mathbb{Z}_p)} \zeta_\psi^{x/y}\,d\beta(x) = 0 . \tag{3.9}$$

Let $t \in 1 + p^{n_0}\mathbb{Z}_p$. Replacing y by yt in (3.9) and then applying σ_t gives

$$\int_{yt(1+p^n\mathbb{Z}_p)} \zeta_\psi^{x/y}\,d\beta(x) = 0 , \tag{3.10}$$

and summing (3.10) over a complete set of representatives

$t \in 1 + p^{n_o}\mathbb{Z}_p$ for $(1 + p^{n_o}\mathbb{Z}_p) / (1 + p^n\mathbb{Z}_p)$, we obtain the final formula of the lemma.

We may now complete the proof of Theorem 3.2 as follows. Assume that $\Gamma_\alpha(\psi) = 0$ for infinitely many ψ. Fix $y \in U$ for the moment. By Lemma 3.6, $\hat{\beta}_y$ has infinitely many zeros in μ_{p^∞}. Now, by (3.4) and (1.7),

$$\beta_y = \beta|_{y(1 + p^{n_o}\mathbb{Z}_p)} = \sum_{\eta \in V} \alpha\circ\eta \;|_{y(1 + p^{n_o}\mathbb{Z}_p)} , \tag{3.11}$$

$$= \sum_\eta (\alpha|_{\eta y(1 + p^{n_o}\mathbb{Z}_p)}) \circ\eta .$$

Since α is a rational function measure, so is $\alpha|_{\eta y(1 + p^{n_o}\mathbb{Z}_p)}$ by (1.16); let $R_{\eta y}(Z)$ be the rational function associated to $\alpha|_{\eta y(1+p^{n_o}\mathbb{Z}_p)}$.

Then, by (3.11) and (1.10),

$$\hat{\beta}_y(\zeta) = \sum_\eta R_{\eta y}(\zeta^{1/\eta}) = 0 \tag{3.12}$$

for infinitely many $\zeta \in \mu_{p^\infty}$.

Let A be the additive subgroup of $\mathbb{Z}_p$ generated by the elements of V, and let $a_1,\dots,a_n$ be a $\mathbb{Z}$ - basis for A. Let

$$h\colon \overline{\mathbb{F}}_\ell(X_1,\dots,X_n) \to \mathcal{F}_0.$$

be the inclusion induced, as in Corollary 2.4, by sending X_i to z^{a_i}. Let $\eta_1,\dots,\eta_m$ be a complete set of representatives in V for $V/\{\pm 1\}$; if we write

$$1/\eta_j = \sum_{i=1}^{n} c_{ij}\, a_i , \quad c_{ij} \in \mathbb{Z} , \; j=1,\dots,m,$$

and let

$$Y_j = \prod_{i=1}^{n} X_i^{c_{ij}},$$

then $h(Y_j) = z^{1/n_j} \in \mathcal{F}_0$. Let

$$F(X_1,\ldots,X_n) = \sum_{j=1}^{m} R_{n_j y}(Y_j) + R_{-n_j y}(Y_j^{-1}) \in \overline{\mathbb{F}}_\ell(X_1,\ldots,X_n),$$

and view $\hat{\beta}_y$ as an element of $\mathcal{F}_0$. By (3.12), $h(F) = \hat{\beta}_y$ has infinitely many zeros; so $h(F)$ is not a unit in $\mathcal{F}_0$; so $h(F) = 0$ and $F = 0$. Since the Y_j's are pairwise multiplicatively independent over $\mathbb{Z}$, it follows from Proposition 3.1 of [1] (see appendix) that

$$R_{n_j y}(Z) + R_{-n_j y}(Z^{-1}) \in k, \tag{3.13}$$

for $j = 1,\ldots,m$, and also, replacing Z by Z^{-1} in (3.13),

$$R_{-n_j y}(Z) + R_{n_j y}(Z^{-1}) \in k, \tag{3.14}$$

for $j = 1,\ldots,m$. Adding (3.13) to (3.14) and summing over j and over a complete set of representatives $y \in U$ for $U/(1+p^{n_0}\mathbb{Z}_p)$ we obtain

$$R(Z) + R(Z^{-1}) \in k .$$

However, the identity (1.18) implies that we must in fact have $R(Z) + R(Z^{-1}) = 0$. This completes the proof of Theorem 3.2.

§4. Washington's Theorem.

4.1. Notations: Let $\mathbb{Q}_\ell$ denote the field of ℓ-adic numbers, $\overline{\mathbb{Q}}_\ell$ a fixed algebraic closure of $\mathbb{Q}_\ell$, $\mathbb{Z}_\ell$ the ℓ-adic integers, and $\overline{\mathbb{Z}}_\ell$ the integral closure of $\mathbb{Z}_\ell$ in $\overline{\mathbb{Q}}_\ell$; we identify the residue field of $\overline{\mathbb{Z}}_\ell$ with $\overline{\mathbb{F}}_\ell$ and denote the natural reduction map $\overline{\mathbb{Z}}_\ell \to \overline{\mathbb{F}}_\ell$ by $\sim$. We let ord_ℓ denote the usual valuation on $\overline{\mathbb{Q}}_\ell$, normalized by $\mathrm{ord}_\ell(\ell) = 1$.

If F is an abelian extension of $\mathbb{Q}$, not necessarily finite, then by a character of $F/\mathbb{Q}$ we mean a character of finite order of $\mathrm{Gal}(F/\mathbb{Q})$ with values in $\overline{\mathbb{Q}}_\ell^\times$. If χ is such a character, the primitive Dirichlet character associated to χ by class field theory will also be denoted by χ. Let f be any multiple of the conductor of χ and define

$$(4.2) \qquad F_\chi(Z) = \frac{\sum_{a=1}^{f} \chi(a) Z^a}{1 - Z^f} \in \overline{\mathbb{Q}}_\ell(Z) ;$$

F_χ does not depend on the particular choice of f. According to Hurwitz, we have, for nontrivial χ,

$$(4.3) \qquad L(0,\chi) = F_\chi(1) .$$

Here $L(0,\chi)$ is defined to be $L(0,\chi^\sigma)^{\sigma^{-1}}$, where $\sigma: \overline{\mathbb{Q}}_\ell \tilde{\to} \mathbb{C}$ is an arbitrary field isomorphism and $L(s,\chi^\sigma)$ denotes the Dirichet L-function attached to χ^σ. $L(0,\chi)$ is independent of the choice of σ.

4.4. Washington's Theorem: In [2], Washington reduced his then conjectural theorem on class numbers (described in the introduction above) to the following assertion about the numbers $L(0,\chi)$, subsequently proved by him in [3]:

Fix an odd character θ of $\mathbb{Q}^{ab}/\mathbb{Q}$ of finite order and values in $\overline{\mathbb{Q}}_\ell$, and let ψ vary through the characters of $\mathbb{Q}_\infty/\mathbb{Q}$ with values in $\overline{\mathbb{Q}}_\ell$ (here $\mathbb{Q}_\infty/\mathbb{Q}$ is the $\mathbb{Z}_p$-extension of $\mathbb{Q}$). Then

$$\operatorname{ord}_\ell \frac{1}{2} L(0,\theta\psi) = 0$$

for almost all such characters ψ.

4.5. Values of L-Functions and Γ-Transforms: We now show how to derive the assertion of (4.4) from Theorem 3.2 above. We fix from now on an odd character θ of $\mathbb{Q}^{ab}/\mathbb{Q}$. The following proposition is essentially well-known:

Proposition 4.6 Let f_0 be the conductor of θ, and let $f = 2pf_0$. Let

$$R(Z) = \frac{\sum_{a=1,\, p\nmid a}^{f/2} \theta(a) Z^a}{1 - Z^f}.$$

Then for any character ψ of $\mathbb{Q}_\infty/\mathbb{Q}$ whose conductor p^m does not divide f, we have

$$\frac{1}{2} L(0,\theta\psi) = \sum_\zeta{}' \tau(\psi,\zeta) R(\zeta),$$

the summation taken over primitive p^m-th roots of unity ζ in $\overline{\mathbb{Q}}_\ell$. Here

$$\tau(\psi,\zeta) = \frac{1}{p^m} \sum_{\substack{a \bmod p^m \\ p\nmid a}} \psi(a)\, \zeta^{-a} \tag{4.7}$$

Proof. Let $\sum_\zeta{}'$ denote summation over the primitive p^m-th roots of unity in $\overline{\mathbb{Q}}_\ell$.

To begin with, we note the following identities:

$$(4.8)\qquad R(Z) + R(Z^{-1}) = \frac{\sum_{a=1,\ p\nmid a}^{f} \theta(a)Z^a}{1 - Z^f} = \frac{\sum_{a=1,p\nmid a}^{fp^m} \theta(a)Z^a}{1 - Z^{fp^m}},$$

so that, if ζ is a primitive p^m-th root of 1 ,

$$(4.9)\qquad R(\zeta) + R(\zeta^{-1}) = \left.\frac{\sum_{a=1,p\nmid a}^{fp^m} \theta(a)\zeta^a Z^a}{1 - Z^{fp^m}}\right|_{Z=1} .$$

Also, for any integer a prime to p,

$$(4.10)\qquad \sum_{\zeta}{}' \tau(\psi,\zeta)\zeta^a = \psi(a) ;$$

for this it is helpful to notice that $\tau(\psi,\zeta)$, defined by (4.7), is 0 if ζ is an imprimitive p^m-th root of unity, so the sum may be extended over all p^m-th roots of unity ζ .

Now, since ψ is even, we have $\tau(\psi,\zeta) = \tau(\psi,\zeta^{-1})$; hence

$$\begin{aligned} 2\sum_{\zeta} \tau(\psi,\zeta)R(\zeta) &= \sum_{\zeta}{}' (\tau(\psi,\zeta) + \tau(\psi,\zeta^{-1}))R(\zeta) \\ &= \sum_{\zeta}{}' \tau(\psi,\zeta)(R(\zeta) + R(\zeta^{-1})) \\ &= \left.\frac{\sum_{a=1,p\nmid a}^{fp^m} \theta(a)\psi(a)Z^a}{1 - Z^{fp^m}}\right|_{Z=1} , \end{aligned}$$

by (4.9) and (4.10). Since $p^m \nmid f$, the conductor of $\theta\psi$ is divisible by p, and this reduces to

$$\left. \frac{\sum_{a=1}^{fp^m} \Theta\psi(a) Z^a}{1 - Z^{fp^m}} \right|_{Z=1} = L(0,\Theta\psi) \quad ,$$

by (4.2). This completes the proof of the proposition.

Now let $\tilde{R}(Z)$ denote the rational function in $\bar{\mathbb{F}}_\ell(Z)$ obtained from $R(Z)$ by applying $\sim$ to its coefficients. By (1.8) we can determine a measure α on $\mathbb{Z}_p$ with values in $\bar{\mathbb{F}}_\ell$ by stipulating that

$$\hat{\alpha}(\zeta) = \tilde{R}(\zeta) \; ,$$

for $\zeta \in \mu_{p^\infty}$ for which $\zeta^f \neq 1$ and setting $\hat{\alpha}(\zeta) = 0$ otherwise. Then α is supported on $\mathbb{Z}_p^\times$, by (1.17). If $\psi \in \Phi$ (1.11), let ψ' be the character of $\mathbb{Q}_\infty/\mathbb{Q}$ which satisfies

$$\psi'(a)^\sim = \psi(a) \; ,$$

for integers a prime to p; on the right we are viewing ψ as a character of $\mathbb{Z}_p^\times$ trivial on V, as in (1.11). Then $\tau(\psi',\zeta)^\sim = \tau(\psi,\zeta)$, as defined by (4.7) and (1.14), respectively; hence, by (1.15) and Proposition (4.6), we have

$$\Gamma_\alpha(\psi) = (\tfrac{1}{2} L(0,\Theta\psi'))^\sim \; ,$$

if the conductor of ψ' does not divide f. Now $\tilde{R}(Z) + \tilde{R}(Z^{-1}) \neq 0$, by (4.8); hence $\Gamma_\alpha(\psi) = 0$ for only finitely many ψ, by Theorem 3.2. Thus the assertion of (4.4) follows.

Appendix

We recall here Proposition 3.1 of [1] and sketch a different proof:

Let k be a field, $X_1,\ldots,X_n,Z$ $(n \geq 1)$ independent indeterminates over k, and $Y_1,\ldots,Y_m$ $(m \geq 1)$ nontrivial elements of the multiplicative group $M = \prod_{i=1}^{n} X_i^{\mathbb{Z}}$ generated by $X_1,\ldots,X_n$ in $k(X_1,\ldots,X_n)^{\times}$. Suppose that the Y_j's are pairwise multiplicatively independent, i.e. $Y_i^a = Y_j^b$ with $i \neq j$ only if $a = b = 0$. Then a relation of the form

$$(*) \qquad r_1(Y_1) + \ldots + r_m(Y_m) = 0,$$

with $r_j(Z) \in k(Z)$, can occur only if

$$r_j(Z) \in k, \quad j = 1,\ldots,m.$$

Sketch of proof: Let $R = k[X_1,\ldots,X_m, X_1^{-1},\ldots,X_m^{-1}]$; then R is a unique factorization domain and $R^{\times} = k^{\times}\cdot M$. If $f(Z)$, $g(Z)$ are non-zero polynomials in $k[Z]$ and $i \neq j$, one can check that $f(Y_i)$ and $g(Y_j)$ are relatively prime in R.

Let $r_i(Z) = f_j(Z)/g_j(Z)$, where f_i, g_j are polynomials over k. Since the elements $g_j(Y_j)$, $j = 1,\ldots,m$, are relatively prime in R, (*) implies that $g_i(Z)$ has the form aZ^b, $a \in k^{\times}$, $b \in Z$. Hence each $r_j(Z)$ is a "Laurent polynomial", i.e. $r_j(Z) \in k[Z,Z^{-1}]$, and $r_j(Y_i) \in k[Y_j, Y_j^{-1}] \subsetneq R$. Since each element of R can be written uniquely as a k-linear combination of elements of M, (*) implies that each $r_j(Z)$ is a constant, since for each j and $a \neq 0$, the element $Y_j^a \in M$ occurs at most once on the left-hand side of (*), and hence not at all.

REFERENCES:

1. Sinnott, W.: On the μ-invariant of the Γ-transform of a rational function. Invent. Math. 75, 273 - 282 (1984).

2 Washington, L.: Class numbers and $\mathbb{Z}_p$-extensions, Math. Ann. 214, 177 - 193 (1975).

3. Washington, L.: The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension. Invent. Math 49, 87 - 97 (1978)

Warren Sinnott
Department of Mathematics
The Ohio State University
Columbus, Ohio 43210
U.S.A.