COMPOSITIO MATHEMATICA

HIROO MIKI

On the conductor of the Jacobi sum Hecke character

Compositio Mathematica, tome 92, nº 1 (1994), p. 23-41
<http://www.numdam.org/item?id=CM_1994__92_1_23_0>

Compositio Mathematica **92**: 23–41, 1994.

On the conductor of the Jacobi sum Hecke character*

HIROO MIKI

Institut des Hautes Etudes Scientifiques, 91440 Bures-sur-Yvette, France and Department of Liberal Arts and Sciences, Faculty of Engineering and Design, Kyoto Institute of Technology, Sakyo-ku, Kyoto 606, Japan

Received 28 August 1992; accepted in final form 10 April 1993

Recently, Coleman-McCallum [5] determined completely the precise conductor of the Jacobi sum Hecke character, using the stable reduction of Fermat curves.

In this paper, we will give a purely number theoretic proof of their results (see Theorem 3 and its Corollary in the present paper), not using the geometry of Fermat curves. Our proof is much simpler than theirs.

First, we give the definition of the Jacobi sum.

DEFINITION. For arbitrary positive integers m, r and any $a = (a_1, \dots, a_r) \in \mathbb{Z}^r$ and for any prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\zeta_m)$ which is prime to m, put

$$J_m^{(a)}(\mathfrak{p}) = (-1)^{r+1} \sum_{\substack{x_1 + \cdots + x_r = -1 \\ x_1, \dots, x_r \in \mathbb{Z}[\zeta_m]/\mathfrak{p}}} \chi_{\mathfrak{p}}^{a_1}(x_1)\chi_{\mathfrak{p}}^{a_2}(x_2)\cdots\chi_{\mathfrak{p}}^{a_r}(x_r) \in \mathbb{Z}[\zeta_m],$$

where $\mathbb{Q}$ is the field of rational numbers, $\mathbb{Z}$ is the ring of rational integers, $\zeta_m \in \mathbb{C}$ (the field of complex numbers) is a primitive mth root of unity, and $\chi_{\mathfrak{p}}(x) = (x/\mathfrak{p})_m$ is the mth power residue symbol in $\mathbb{Q}(\zeta_m)$, i.e. $\chi_{\mathfrak{p}}(x \bmod \mathfrak{p})$ is a unique mth root of unity in $\mathbb{C}$ such that

$$\chi_{\mathfrak{p}}(x \bmod \mathfrak{p}) \equiv x^{(N\mathfrak{p}-1)/m} \pmod{\mathfrak{p}}$$

for $x \in \mathbb{Z}[\zeta_m], \notin \mathfrak{p}$. Here $N\mathfrak{p}$ is the number of elements in $\mathbb{Z}[\zeta_m]/\mathfrak{p}$. Put $\chi_{\mathfrak{p}}(0) = 0$. For any fractional ideal $\mathfrak{a}$ of $\mathbb{Q}(\zeta_m)$ which is prime to m, put

$$J_m^{(a)}(\mathfrak{a}) = \prod_{\mathfrak{p}} J_m^{(a)}(\mathfrak{p})^{e_{\mathfrak{p}}},$$

where $\mathfrak{a} = \Pi_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ is the prime ideal decomposition of $\mathfrak{a}$. $J_m^{(a)}(\mathfrak{a})$ is called the *Jacobi sum.*

*This paper is the details of a part of my talk in *Number Theory Seminar* (Goldfeld), Columbia University, March 21, 1988 (see [16]).

By Weil [23], $J_m^{(a)}(\mathfrak{a})$ is a Hecke character of $\mathbb{Q}(\zeta_m)$ as a function in $\mathfrak{a}$ with conductor $C_m^{(a)}$ dividing m^2. He raised the problem of giving the precise value of the conductor $C_m^{(a)}$. The Jacobi sum is an interesting Hecke character and it is a natural problem to give the precise conductor for a given Hecke character. Hasse [6] determined the precise $C_m^{(a)}$ when $r = 2$ and $m = l$ is any odd prime number. Iwasawa [11] determined (essentially) the precise $C_m^{(a)}$ when $r \geqslant 2$ and $m = l$ is any odd prime number. Jensen [12] and Schmidt [20] gave certain estimates for $C_m^{(a)}$. Rohrlich [19] proved that $C_m^{(a)} | (\zeta_l - 1)^2$ when $r = 2$ and $m = l^n$ with any integer $n \geqslant 1$ and any odd prime l, by using Artin-Hasse's and Iwasawa's explicit formulas for the Hilbert norm residue symbol [2], [8]. Miki [15] gave the precise $C_m^{(a)}$ when $r \geqslant 2$ and $m = l^2$ with any odd prime l, by using a congruence for the Jacobi sum [14] which generalizes Hasse-Iwasawa-Ihara's [6], [7], [11]. The method of [15] can be regarded as a generalization of Hasse's [6] and Iwasawa's [11]. Coleman-McCallum [5] gave a complete solution of the problem by using the stable reduction of Fermat curves and Shimura-Taniyama's complex multiplication of abelian varieties [21]. We should also note that Coleman ([4], Section VI) (with G. Anderson) gave another proof (at least under the assumption $(l, a_0 a_1 \cdots a_r) = 1$) as an application of Ihara [7] and Anderson [1], and that Kato [13] gave another proof as an application of his theory.

The present paper can be regarded as a generalization of Rohrlich [19] and Miki [15], and the main idea is to use the homomorphism $\delta^{(n)}$ of $U_n^{(1)}$ (the group of principal units) to $\mathcal{O}_K / l^n \mathcal{O}_K$ which is related to Artin-Hasse's and Iwasawa's explicit formulas for the Hilbert norm residue symbol (see Lemma 1 in Section 1), instead of using the congruence for the Jacobi sum.

Our number theoretic proof involves the calculation of the Hilbert symbol $(1 + l, J_{l^n}^{(a)}(\mathfrak{a}))_n$ and that of certain sums $W_n(a)$ and $S_{l^n}^{(a)}$ (see Theorems 1 and 2, and corollary to Theorem 2), which are new results not contained in Coleman-McCallum [5]. The determination of the conductor follows directly from those calculations (see Theorem 3 and its corollary).

1. Certain homomorphism $\delta^{(n)}$ of $U_n^{(1)}$ to $\mathcal{O}_K / l^n \mathcal{O}_K$ and the calculation of $\delta^{(n)}(J_{l^n}^{(a)}(\mathfrak{a}))$

Let l be an odd prime number† and let n be a positive integer. Let $\mathbb{Z}_l$ and $\mathbb{Q}_l$ denote the ring of l-adic integers and the field of l-adic numbers respectively. We fix an algebraic closure $\bar{\mathbb{Q}}_l$ of $\mathbb{Q}_l$ once for all, and we consider that all algebraic extensions of $\mathbb{Q}_l$ and all elements which are algebraic over $\mathbb{Q}_l$ are

†Though almost all parts of the present paper are valid for $l = 2$ with slight modification, we will discuss in the case $l = 2$ elsewhere.

contained in $\bar{\mathbb{Q}}_l$. All congruences in the present paper are those in $\bar{\mathbb{Q}}_l$. Fix a sequence $\zeta_l, \zeta_{l^2}, \ldots, \zeta_{l^i}, \zeta_{l^{i+1}}, \ldots$ of a primitive l^ith root of unity such that $\zeta_{l^{i+1}}^l = \zeta_{l^i}$ for $i = 1, 2, 3, \ldots$ and put $\pi_i = 1 - \zeta_{l^i}$. Fix any finite unramified extension K of $\mathbb{Q}_l$ and let $\mathcal{O}_K$ be the ring of integers of K. Put $K_n = K(\zeta_{l^n})$ and $K_\infty = \bigcup_{i=1}^\infty K_i$. Then $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_l^\times$ (the group of units in $\mathbb{Z}_l$) by $\sigma_a \leftrightarrow a$, where $\sigma_a \in \mathrm{Gal}(K_\infty/K)$ is such that $\zeta_{l^i}^{\sigma_a} = \zeta_{l^i}^a$ for all $i \geqslant 1$. Put

$$\delta^{(n)}(\alpha) = \frac{-1}{l^{n-1}(l-1)} \mathrm{Tr}_{K_n/K}\left(\zeta_{l^n}\alpha^{-1}\frac{\mathrm{d}\alpha}{\mathrm{d}\pi_n}\right) \quad \text{for } \alpha \in U_n^{(1)},$$

where $U_n^{(1)}$ is the group of principal units in K_n:

$$U_n^{(1)} = \{x \in \mathcal{O}_{K_n}^\times \mid x \equiv 1 \pmod{\pi_n}\},$$

$\mathrm{Tr}_{K_n/K}$ is the trace from K_n to K, and $\mathrm{d}\alpha/\mathrm{d}\pi_n = f'(\pi_n)$. Here $f(T)$ is a formal power series in T with coefficients in $\mathcal{O}_K$ satisfying $\alpha = f(\pi_n)$, and $f'(T)$ is the formal derivative of $f(T)$ with respect to T. Let $[\alpha, \beta]_n \in \mathbb{Z}/l^n\mathbb{Z}$ be such that $(\alpha, \beta)_n = \zeta_{l^n}^{[\alpha,\beta]_n}$ for α, $\beta \in \mathbb{Q}_l(\zeta_{l^n})^\times$, where $(\alpha, \beta)_n$ is the Hilbert norm residue symbol in $\mathbb{Q}_l(\zeta_{l^n})$ for the power l^n defined by

$$(\alpha, \beta)_n = (\sqrt[l^n]{\beta})^{\rho(\alpha)-1}.$$

Here $\rho\colon \mathbb{Q}_l(\zeta_{l^n})^\times \to \mathrm{Gal}(\mathbb{Q}_l(\zeta_{l^n})^{ab}/\mathbb{Q}_l(\zeta_{l^n}))$ is the Artin map in local class field theory and $\mathbb{Q}_l(\zeta_{l^n})^{ab}$ is the maximum abelian extension of $\mathbb{Q}_l(\zeta_{l^n})$. Then the following Lemma 1 is a direct consequence of Iwasawa [8] (though he assumes $K = \mathbb{Q}_l$, the proof is the same for general K).

LEMMA 1. *Let the notation and assumptions be as above. Then $\delta^{(n)}$ is a well-defined homomorphism of $U_n^{(1)}$ to $\mathcal{O}_K/l^n\mathcal{O}_K$ satisfying the following properties* (i) ~ (v) *for* $\alpha \in U_n^{(1)}$:

(i) $\delta^{(n)}(\alpha^{\sigma_a}) \equiv a\delta^{(n)}(\alpha) \pmod{l^n\mathcal{O}_K}$ *for* $a \in \mathbb{Z}_l^\times$.
(ii) $\delta^{(n)}(\zeta_{l^n}) \equiv 1 \pmod{l^n\mathcal{O}_K}$.
(iii) $\delta^{(n)}(\alpha) \equiv -c\ [1 + l, \alpha]_n \pmod{l^n\mathcal{O}_K}$ *if* $\alpha \in U_n^{(1)} \cap \mathbb{Q}_l(\zeta_{l^n})$, *where* $c = ((1 - 1/l)\log(1 + l))^{-1} \in \mathbb{Z}_l^\times$ *and* log *is the l-adic logarithm.*
(iv) $\delta^{(n)}(\alpha) \equiv 0 \pmod{l^n\mathcal{O}_K}$ *if* $\alpha \equiv 1 \pmod{\pi_1^2}$ *and* $\alpha \in \mathbb{Q}_l(\zeta_{l^n})$.
(v) $\delta^{(n+1)}(\alpha') \equiv \delta^{(n)}(N_{n+1,n}(\alpha')) \pmod{l^n\mathcal{O}_K}$ *if* $\alpha' \in U_{n+1}^{(1)}$, *where* $N_{n+1,n}$ *is the norm map of* K_{n+1} *to* K_n.

REMARK. (i) In [16], we used the Coates-Wiles homomorphism [3] to prove the existence of a homomorphism satisfying the above properties (i) ~ (v) of Lemma 1, but here we adopt a more direct method using Iwasawa [8]. For the details of the relation between $\delta^{(n)}$ and the Coates-Wiles homomorphism, we will discuss elsewhere.

(ii) Conversely, if $K = \mathbb{Q}_l$, then we can define $\delta^{(n)}$ by $\delta^{(n)}(\alpha) = -c[1+l,\alpha]_n$ for $\alpha \in U_n^{(1)}$. Then the property (i) of Lemma 1 is a well-known property of the norm residue symbol, and the property (ii) of Lemma 1 is one of Artin-Hasse's explicit formulas for the norm residue symbol [2]. Once we determine the value of $[1+l, J_{l^n}^{(a)}(\mathfrak{a})]_n$, the homomorphism $\delta^{(n)}$ only for $K = \mathbb{Q}_l$ and only the properties (i) and (ii) of Lemma 1 are sufficient for our proof of Theorem 3, but it is crucial for our calculation of $[1+l, J_{l^n}^{(a)}(\mathfrak{a})]_n$ to define $\delta^{(n)}$ for any finite unramified extension K of $\mathbb{Q}_l$ (see the proof of Theorem 1).

(iii) We do not use the property (v) in Lemma 1 in the present paper.

Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. We consider that all algebraic extensions of $\mathbb{Q}$ and all elements algebraic over $\mathbb{Q}$ are contained in $\bar{\mathbb{Q}}$. By a fixed imbedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_l$, we consider $\bar{\mathbb{Q}}$ as a subfield of $\bar{\mathbb{Q}}_l$.

For any positive integer m and any $a \in \mathbb{Z}$, put

$$g_m(\mathfrak{p}, a) = -\sum_{x \in \mathbb{Z}[\zeta_m]/\mathfrak{p}} \chi_{\mathfrak{p}}^a(x)\psi_{\mathfrak{p}}(x) \in \mathbb{Z}[\zeta_{mp}],$$

where $\psi_{\mathfrak{p}}(x) = \zeta_p^{T(x)}$ (p is a prime number such that $p \in \mathfrak{p}$ and T is the trace of $\mathbb{Z}[\zeta_m]/\mathfrak{p}$ to $\mathbb{Z}/p\mathbb{Z}$), and put

$$g_m(\mathfrak{a}, a) = \prod_{\mathfrak{p}} g_m(\mathfrak{p}, a)^{e_{\mathfrak{p}}} \quad \text{and} \quad g_m(\mathfrak{a}) = g_m(\mathfrak{a}, 1),$$

where $\mathfrak{a} = \Pi \mathfrak{p}^{e_{\mathfrak{p}}}$ is the prime ideal decomposition of any fractional ideal $\mathfrak{a}$ of $\mathbb{Q}(\zeta_m)$ which is prime to m. This is called the *Gauss sum*. Clearly $g_m(\mathfrak{a}\mathfrak{b}, a) = g_m(\mathfrak{a}, a)g_m(\mathfrak{b}, a)$. It is well known that if $a = (a_1, \ldots, a_r) \not\equiv (0, \ldots, 0) \pmod m$, then

$$J_m^{(a)}(\mathfrak{a}) = N\mathfrak{a}^{-1} \cdot \prod_{i=0}^{r} g_m(\mathfrak{a}, a_i), \tag{1}$$

where

$$a_0 = -\sum_{i=1}^{r} a_i.$$

Now assume $m = l^n$ and the following condition (*) on K and $\mathfrak{a}$:

$$K \ni \zeta_p \textit{ for any prime number } p \textit{ contained in any prime ideal dividing } \mathfrak{a}. \tag{*}$$

Then $g_{l^n}(\mathfrak{a}, a) \in K_n$. By the following Lemma 2, we can see the action of the Galois group $\mathrm{Gal}(K_n/\mathbb{Q}_l) = \mathrm{Gal}(K_n/K) \times \mathrm{Gal}(K_n/\mathbb{Q}_l(\zeta_{l^n}))$ (direct product) on $g_{l^n}(\mathfrak{a}, a)$.

LEMMA 2. *Under the above assumption* (*), *we have the following*:

(i) $g_{l^n}(\mathfrak{a}, a)^{\sigma_c} = g_{l^n}(\mathfrak{a}, ac)$ *for* $c \in \mathbb{Z}_l^\times$.
(ii) $g_{l^n}(\mathfrak{a}, a)^\tau = \zeta_{l^n}^{-\langle l,\mathfrak{a}\rangle a} g_{l^n}(\mathfrak{a}, a)$, *where* $\tau \in \mathrm{Gal}(K_n/\mathbb{Q}_l(\zeta_{l^n}))$ *is the Frobenius automorphism, and* $\langle x, \mathfrak{a}\rangle \in \mathbb{Z}/l^n\mathbb{Z}$ *is defined by* $(x/\mathfrak{a})_{l^n} = \zeta_{l^n}^{\langle x,\mathfrak{a}\rangle}$.

Proof. It suffices to prove for $\mathfrak{a} = \mathfrak{p}$. Since (i) is trivial, we prove (ii). Since τ acts trivially on $\chi_\mathfrak{p}^a(x)$,

$$g_{l^n}(\mathfrak{p}, a)^\tau = - \sum_{x \in \mathbb{Z}[\zeta_{l^n}]/\mathfrak{p}} \chi_\mathfrak{p}^a(x)\psi_\mathfrak{p}(x)^\tau,$$

so

$$\begin{aligned} g_{l^n}(\mathfrak{p}, a)^\tau &= -\sum_x \chi_\mathfrak{p}^a(x)\psi_\mathfrak{p}(xl) \\ &= \chi_\mathfrak{p}(l)^{-a} g_{l^n}(\mathfrak{p}, a), \end{aligned}$$

hence we have the assertion.

For $a \in \mathbb{Z}$, we write $a = a'a''$, where a' is the power of l and $a'' \in \mathbb{Z}$ is prime to l. If $a = 0$, then put $a' = 0$ and $a'' = 1$. Under this notation, we have the following congruence (mod l) for the Gauss sum $g_{l^n}(\mathfrak{a}, a)$ and the Jacobi sum $J_{l^n}^{(a)}(\mathfrak{a})$:

LEMMA 3. *Under the assumption* (*) *before Lemma* 2, *we have the following congruences*:

(i) $g_{l^n}(\mathfrak{a}, a^{l^j}) \equiv \zeta_{l^n}^{\langle l^j,\mathfrak{a}\rangle a l^j} g_{l^n}(\mathfrak{a}, a)^{l^j} \pmod{l}$ *for* $a, j \in \mathbb{Z}, j \geqslant 1$.
(ii) $g_{l^n}(\mathfrak{a}, a) \equiv \zeta_{l^n}^{\langle l,\mathfrak{a}\rangle(\mathrm{ord}_l(a)\cdot a)} g_{l^n}(\mathfrak{a})^{a'\sigma_{a''}} \pmod{l}$ *for* $a \in \mathbb{Z}$, *where* ord_l *is the normalized additive valuation of* $\mathbb{Q}_l$, *and* $\mathrm{ord}_l(0)\cdot 0 = \infty \cdot 0 = 0$.
(iii) $J_{l^n}^{(a)}(\mathfrak{a}) \equiv N\mathfrak{a}^{-1} \cdot \zeta_{l^n}^{\langle l,\mathfrak{a}\rangle g} g_{l^n}(\mathfrak{a})^\omega \pmod{l}$ *if* $a = (a_1, \ldots, a_r) \not\equiv (0, \ldots, 0) \pmod{l^n}$, *where* $a_0 = -\Sigma_{i=1}^r a_i$, $g = \Sigma_{i=0}^r \mathrm{ord}_l(a_i)\cdot a_i$, $\omega = \Sigma_{i=0}^r a_i'\sigma_{a_i''} \in \mathbb{Z}[\mathrm{Gal}(K_n/K)]$ (*the group ring of* $\mathrm{Gal}(K_n/K)$ *over* $\mathbb{Z}$).

Proof. It is sufficient to prove for $\mathfrak{a} = \mathfrak{p}$.

(i) Put $a_1 = al^j$. Then

$$\begin{aligned} g_{l^n}(\mathfrak{p}, a)^{l^j} &= \left(-\sum_x \chi_\mathfrak{p}^a(x)\psi_\mathfrak{p}(x)\right)^{l^j} \\ &\equiv -\sum_x \chi_\mathfrak{p}^{a_1}(x)\psi_\mathfrak{p}(l^j x) \pmod{l} \\ &\equiv \chi_\mathfrak{p}^{-a_1}(l^j) g_{l^n}(\mathfrak{p}, a_1) \pmod{l} \\ &\equiv \zeta_{l^n}^{-\langle l^j,\mathfrak{p}\rangle a_1} g_{l^n}(\mathfrak{p}, a_1) \pmod{l} \end{aligned}$$

by the equality $\psi_{\mathfrak{p}}(x)^{l^j} = \psi_{\mathfrak{p}}(l^j x)$ and the definition of $\langle l^j, \mathfrak{p}\rangle$. Thus we obtain the desired congruence.

(ii) Since the case $a = 0$ is trivial, we may assume $a \neq 0$. We can write $a = a'a''$, where $a' = l^j$, $j = \mathrm{ord}_l(a)$ and $a'' \in \mathbb{Z}$ is prime to l. Then the congruence (ii) is a direct consequence of (i), since $\langle l^j, \mathfrak{p}\rangle \equiv j\langle l, \mathfrak{p}\rangle \pmod{l^n}$ and $g_{l^n}(\mathfrak{p})^{\sigma_{a''}} = g_{l^n}(\mathfrak{p}, a'')$ by (i) of Lemma 2.

(iii) This follows immediately from the congruence (ii) and the equality (1).

By Lemmas 1, 2, and 3, we will determine the value of $\delta^{(n)}(J_{l^n}^{(a)}(\mathfrak{a}))$, i.e., that of $[1 + l, J_{l^n}^{(a)}(\mathfrak{a})]_n$:

THEOREM 1. *If* $a = (a_1, \ldots, a_r) \not\equiv (0, \ldots, 0) \pmod{l^n}$, *then*

$$\delta^{(n)}(J_{l^n}^{(a)}(\mathfrak{a})) \equiv \langle l, \mathfrak{a}\rangle g \pmod{l^n},$$

i.e.

$$[1 + l, J_{l^n}^{(a)}(\mathfrak{a})]_n \equiv -\left(1 - \frac{1}{l}\right) \log(1 + l) \cdot \langle l, \mathfrak{a}\rangle g \pmod{l^n},$$

where $g = \sum_{i=0}^{r} \mathrm{ord}_l(a_i) \cdot a_i$, *and* $\langle l, \mathfrak{a}\rangle$ *is as in Lemma* 2.

Proof. Take $K = \mathbb{Q}_l(\zeta_p \mid p \in P)$, where P is the set of all prime numbers contained in any prime ideal dividing $\mathfrak{a}$. Since

$$(g_{l^n}(\mathfrak{a})^{\omega})^{\tau} = g_{l^n}(\mathfrak{a})^{\omega}$$

by using (ii) of Lemma 2 and the equality $\sum_{i=0}^{r} a_i = 0$, we have $g_{l^n}(\mathfrak{a})^{\omega} \in \mathbb{Q}_l(\zeta_{l^n})$, hence the congruence (iii) of Lemma 3 implies that

$$J_{l^n}^{(a)}(\mathfrak{a}) = N\mathfrak{a}^{-1} \cdot \zeta_{l^n}^{\langle l, \mathfrak{a}\rangle g} g_{l^n}(\mathfrak{a})^{\omega} \cdot \xi \tag{2}$$

with $\xi \in \mathbb{Q}_l(\zeta_{l^n})$, $\xi \equiv 1 \pmod{l}$. Clearly $N\mathfrak{a} \equiv 1 \pmod{l^n}$ and $g_{l^n}(\mathfrak{a}) \in U_n^{(1)}$. Taking $\delta^{(n)}$ of both members of (2), we have immediately the assertion, since

$$\delta^{(n)}(N\mathfrak{a}^{-1}) \equiv \delta^{(n)}(\xi) \equiv 0 \pmod{l^n}$$

by (iv) of Lemma 1,

$$\delta^{(n)}(\zeta_{l^n}^{\langle l, \mathfrak{a}\rangle g}) \equiv \langle l, \mathfrak{a}\rangle g \pmod{l^n}$$

by (ii) of Lemma 1, and

$$\delta^{(n)}(g_{l^n}(\mathfrak{a})^{\omega}) = \left(\sum_{i=0}^{r} a_i' a_i''\right) \delta^{(n)}(g_{l^n}(\mathfrak{a})) = 0$$

by (i) of Lemma 1 and the equality $\Sigma_{i=0}^{r} a_i = 0$.

2. Calculation of a certain sum $S_{l^n}^{(a)}$

For $a \in \mathbb{Z}$, put

$$W_n(a) = \sum_{\substack{0<t<l^n \\ (t,l)=1}} \left(\left\{\frac{at}{l^n}\right\} - a\left\{\frac{t}{l^n}\right\}\right)(-t)^{-1} \in \mathbb{Z}_l,$$

where $\{x\}$ is the fractional part of $x \in \mathbb{Q}$, i.e. $0 \leqslant \{x\} < 1$ such that $\{x\} \equiv x (\mathrm{mod}\, \mathbb{Z})$.

In this section, we will calculate $W_n(a)$ (see Theorem 2 below), and as its corollary, we will get the value of a certain sum $S_{l^n}^{(a)}$, which we need for our proof of Theorem 3.

If $(a, l) = 1$, then the calculation of $W_n(a)$ was made by Iwasawa (see his formula in the line 2, p. 82 of [10]; replace $(1 + q_0)$ and a in the formula by a and t in our notation respectively):

LEMMA 4. *If* $a \in \mathbb{Z}$, $(a, l) = 1$, *then*

$$W_n(a) \equiv \left(1 - \frac{1}{l}\right) \log\langle a\rangle^a \ (\mathrm{mod}\ l^n),$$

where log *is the l-adic logarithm and* $\langle a\rangle$ *is a unique element in* $\mathbb{Z}_l^{\times}$ *such that* $\langle a\rangle \equiv 1 \ (\mathrm{mod}\, l)$ *and* $a/\langle a\rangle$ *is an* $(l-1)$th *root of unity.*

REMARK. By Iwasawa's construction of the l-adic L-function [9],

$$g_a((1 + l)^s - 1) = (\omega(a)\langle a\rangle^s - a)L_l(s, 1),$$

where $\omega(a) = a/\langle a\rangle$ and $g_a(T)$ is the unique power series in T with coefficients in $\mathbb{Z}_l$ satisfying

$$g_a(T) \equiv \sum_{\substack{0<t<l^n \\ (t,l)=1}} \left(a\left\{\frac{t}{l^n}\right\} - \left\{\frac{at}{l^n}\right\}\right)\omega^{-1}(t)(1 + T)^{-i(t)} \quad (\mathrm{mod}\,(1 + T)^{l^n} - 1)$$

for all $n \geqslant 1$. Here $i(t) = \log\langle t\rangle/\log(1+l)$. Hence

$$g_a(l) \equiv W_n(a) \pmod{l^n} \quad \text{and} \quad W_n(a) \equiv \lim_{s\to 1} (\omega(a)\langle a\rangle^s - a)L_l(s, 1) \pmod{l^n}.$$

Since $L_l(s, 1)$ has a pole of order 1 with residue $(1 - 1/l)$ at $s = 1$, this gives another proof of Lemma 4. This is a method used in [16], but here we adopt a more elementary and direct calculation of Iwasawa (see pp. 81–82 of [10]).

We need the following Lemmas 5, 6 and 7 to generalize Lemma 4 for arbitrary $a \in \mathbb{Z}$.

LEMMA 5. *For* $c \in \mathbb{Z}$, *we have the following* (i) *and* (ii):

(i) *If* $c \geqslant 1$, *then*

$$\sum_{j=0}^{l^n} j^c \equiv \sum_{j=1}^{l^n-1} j^c \equiv \begin{cases} 0 & \pmod{l^n} \quad \text{if } (l-1) \nmid c \\ -l^{n-1} & \pmod{l^n} \quad \text{if } (l-1) \mid c. \end{cases}$$

(ii)

$$\sum_{\substack{0<j<l^n \\ (j,l)=1}} j^c \equiv \begin{cases} 0 & \pmod{l^n} \quad \text{if } (l-1) \nmid c \\ -l^{n-1} & \pmod{l^n} \quad \text{if } (l-1) \mid c. \end{cases}$$

Proof. (i) First, suppose c is odd. Then $(l^n - j)^c \equiv -j^c \pmod{l^n}$, so, by pairing j^c and $(l^n - j)^c$ for $j \in \mathbb{Z}$, $0 \leqslant j < l^n/2$ in the sum, we get the desired congruence. Next, assume c is even. Since $lB_i \in \mathbb{Z}_l$ for all $i \geqslant 0$ by the von Staudt-Clausen (cf. [22], Theorem 5.10), using a well known identity (cf. [22], Proposition 4.1)

$$B_c = \frac{1}{l^n} \sum_{j=1}^{l^n} (l^n)^c B_c\left(\frac{j}{l^n}\right),$$

we have easily a congruence

$$\sum_{j=1}^{l^n} j^c \equiv l^n B_c \pmod{l^n}, \tag{1}$$

where $B_c(X) = \Sigma_{i=0}^{c} \binom{c}{i} B_i X^{c-i}$ and B_i is the ith Bernoulli number. Again, by the von Staudt-Clausen theorem, we have

$$B_c \equiv \begin{cases} 0 & \pmod{\mathbb{Z}_l} \quad \text{if } (l-1) \nmid c, \\ -\dfrac{1}{l} & \pmod{\mathbb{Z}_l} \quad \text{if } (l-1) \mid c \end{cases} \tag{2}$$

By (1) and (2), we have the desired congruence.

(ii) Put $c' = c + l^s(l-1)$ with sufficiently large $s \geqslant n$, then $c' \geqslant 1$ and

$$j^{c'} \equiv \begin{cases} j^c & (\text{mod } l^n) \quad \text{if } l \nmid j, \\ 0 & (\text{mod } l^n) \quad \text{if } l \mid j, \end{cases}$$

since $j^{l^s(l-1)} \equiv 1 \pmod{l^n}$ if $l \nmid j$. Hence

$$\sum_{\substack{0<j<l^n \\ (j,l)=1}} j^c \equiv \sum_{j=1}^{l^n} j^{c'} \pmod{l^n}.$$

By this and (i), we get (ii).

LEMMA 6. *For* $0 \leqslant m \leqslant n-1$, *put*

$$A = \sum_{\substack{0<t<l^n \\ (t,l)=1}} \left(\left\{ \frac{t}{l^{n-m}} \right\} - l^m \left\{ \frac{t}{l^n} \right\} \right) (-t)^{-1} \in \mathbb{Z}_l.$$

Then

$$A \equiv \begin{cases} -l^{n-1} & (\text{mod } l^n) \quad \textit{if } l = 3 \quad \textit{and} \quad m = n-1 \geqslant 1, \\ 0 & (\text{mod } l^n) \quad \textit{otherwise}. \end{cases}$$

Proof. If $m = 0$, then it is trivial, so we may assume $m \geqslant 1$. Put

$$B = \sum_{\substack{0<t<l^n \\ (t,l)=1}} \left\{ \frac{t}{l^{n-m}} \right\} (-t)^{-1}$$

and

$$C = l^m \sum_{\substack{0<t<l^n \\ (t,l)=1}} \left\{ \frac{t}{l^n} \right\} (-t)^{-1}.$$

Then $A = B - C$. We can write

$$t = t_1 + t_2 l^{n-m} \quad \text{with } 0 \leqslant t_1 < l^{n-m}, 0 \leqslant t_2 < l^m.$$

Then $(t, l) = 1$ implies $(t_1, l) = 1$. Since

$$\left\{ \frac{t}{l^{n-m}} \right\} = \frac{t_1}{l^{n-m}},$$

we have

$$\begin{aligned}
B &= -\sum_{t_1,t_2} \frac{t_1}{l^{n-m}} (t_1 + t_2 l^{n-m})^{-1} \\
&= -\frac{1}{l^{n-m}} \sum_{t_1,t_2} \left(1 + \frac{t_2}{t_1} l^{n-m}\right)^{-1} \\
&= -\frac{1}{l^{n-m}} \sum_{t_1,t_2} \sum_{i=0}^{\infty} (-1)^i \left(\frac{t_2}{t_1}\right)^i (l^{n-m})^i \\
&= -\frac{1}{l^{n-m}} \sum_{i=0}^{\infty} (-1)^i \left(\sum_{t_1} t_1^{-i}\right)\left(\sum_{t_2} t_2^i\right) l^{(n-m)i} \\
&= -l^m\left(1 - \frac{1}{l}\right) - \sum_{i=1}^{\infty} (-1)^i \left(\sum_{t_1} t_1^{-i}\right)\left(\sum_{t_2} t_2^i\right) l^{(n-m)(i-1)}.
\end{aligned}$$

Since $C = -l^m(1 - 1/l)$, this implies

$$A = -\sum_{i=1}^{\infty} (-1)^i \left(\sum_{t_1} t_1^{-i}\right)\left(\sum_{t_2} t_2^i\right) l^{(n-m)(i-1)}. \tag{$*$}$$

Since

$$\sum_{t_1} t_1^{-i} \equiv 0 \pmod{l^{n-m-1}}$$

and

$$\sum_{t_2} t_2^i \equiv 0 \pmod{l^{m-1}}$$

by Lemma 5, the ith term of $(*)$ is congruent to 0 modulo $l^{n-m-1} \cdot l^{m-1} \cdot l^{2(n-m)}$, hence, mod l^n for $i \geqslant 3$. In the same way, the first term of $(*)$ is congruent to 0 modulo l^n. Thus we have

$$A \equiv -\left(\sum_{t_1} t_1^{-2}\right)\left(\sum_{t_2} t_2^2\right) l^{n-m} \pmod{l^n}.$$

By this and Lemma 5, we have the desired congruence.

By Lemma 6, we will prove the following Lemma 7, which enables us to reduce the computation of $W_n(a)$ for arbitrary $a \in \mathbb{Z}$ to Lemma 4.

LEMMA 7. *Let* $W_n(a)$ *be as in the beginning of Section* 2, *and let* $a \in \mathbb{Z}$ *be of the* *form* $a = a'l^m$ *with* $a', m \in \mathbb{Z}$, $(a', l) = 1$ *and* $0 \leqslant m \leqslant n-1$. *Then*

$$W_n(a) \equiv \begin{cases} l^m W_n(a') - a \pmod{l^n} & \text{if } l = 3 \text{ and } m = n-1 \geqslant 1, \\ l^m W_n(a') \pmod{l^n} & \text{otherwise.} \end{cases}$$

Proof. If $m = 0$, then it is trivial, so we may assume $m \geqslant 1$. Put

$$D = W_n(a) - l^m W_n(a') \in \mathbb{Z}_l.$$

Then

$$D = \sum_{\substack{0<t<l^n \\ (t,l)=1}} \left(\left\{ \frac{at}{l^n} \right\} - l^m \left\{ \frac{a't}{l^n} \right\} \right) (-t)^{-1}$$

$$\equiv \sum_{t \in (\mathbb{Z}/l^n\mathbb{Z})^\times} \left(\left\{ \frac{at}{l^n} \right\} - l^m \left\{ \frac{a't}{l^n} \right\} \right) (-t)^{-1} \pmod{l^n},$$

since $\{at/l^n\}$ and $\{a't/l^n\}$ are determined by t mod l^n and since $\{at/l^n\} - l^m\{a't/l^n\} \in \mathbb{Z}$. Putting $t' = a't$, we have

$$D \equiv a' \sum_{t' \in (\mathbb{Z}/l^n\mathbb{Z})^\times} \left(\left\{ \frac{l^m t'}{l^n} \right\} - l^m \left\{ \frac{t'}{l^n} \right\} \right) (-t')^{-1} \pmod{l^n},$$

i.e.,

$$D \equiv a'A \pmod{l^n},$$

where A is as in Lemma 6. Thus the assertion follows from Lemma 6.

By Lemmas 4 and 7, we have the following:

THEOREM 2. *Let* $W_n(a)$ *be as in the beginning of Section* 2. *Then for any* $a \in \mathbb{Z}$, *we have*

$$W_n(a) \equiv \begin{cases} \left(1 - \frac{1}{l}\right) \log\langle a \rangle^a - a \pmod{l^n} & \text{if } l = 3 \text{ and } \operatorname{ord}_l(a) = n-1 \geqslant 1, \\ \left(1 - \frac{1}{l}\right) \log\langle a \rangle^a - \frac{a}{l} \pmod{l^n} & \text{if } \operatorname{ord}_l(a) \geqslant n, \\ \left(1 - \frac{1}{l}\right) \log\langle a \rangle^a \pmod{l^n} & \text{otherwise,} \end{cases}$$

where we define $\langle a\rangle$ *by* $\langle a\rangle = \langle a'\rangle$ *for* $a = a'l^m$ *with* $m \geqslant 1$, $a' \in \mathbb{Z}_l^\times$ *and* $\langle 0\rangle = 1$.

Proof. Assume $\mathrm{ord}_l(a) \geqslant n$. Then we have easily

$$W_n(a) \equiv -\frac{a}{l} \pmod{l^n}$$

and

$$\log\langle a\rangle^a \equiv 0 \pmod{l^{n+1}}.$$

Hence we have the assertion in the case $\mathrm{ord}_l(a) \geqslant n$. The proof in the other cases follows from Lemmas 4 and 7.

COROLLARY. *For* $a = (a_1, \ldots, a_r) \in \mathbb{Z}^r$, *put*

$$S_{l^n}^{(a)} = \sum_{\substack{0<t<l^n \\ (t,l)=1}} \left(\sum_{i=0}^{r} \left\{\frac{a_i t}{l^n}\right\}\right)(-t)^{-1} \in \mathbb{Z}_l,$$

where

$$a_0 = -\sum_{i=1}^{r} a_i.$$

Then

$$S_{l^n}^{(a)} \equiv \left(1 - \frac{1}{l}\right) \log\left(\prod_{i=0}^{r} \langle a_i\rangle^{a_i}\right) - T_1 - T_2 \pmod{l^n},$$

where

$$T_1 = \frac{1}{l} \sum_{\substack{\mathrm{ord}_l(a_i)=n \\ 0\leqslant i\leqslant r}} a_i,$$

and

$$T_2 = \begin{cases} \displaystyle\sum_{\substack{\mathrm{ord}_l(a_i)=n-1 \\ 0\leqslant i\leqslant r}} & \textit{if } l = 3 \textit{ and } n \geqslant 2, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Since $\Sigma_{i=0}^{r} a_i = 0$, we have

$$S_{l^n}^{(a)} = \sum_{i=0}^{r} W_n(a_i).$$

Hence the assertion follows directly from Theorem 2.

3. Purely number theoretic proof of Coleman-McCallum's theorems

By Lemma 1, Theorem 1, and Corollary to Theorem 2, we will give another proof of Coleman-McCallum's Theorem 3 below ([5], Theorems 5.3, 7.1 and 7.2 when $m = p^n$ and $x \equiv 1 \pmod{\pi_n}$ in their notation), which gives the precise value of the Jacobi sum $J_{l^n}^{(a)}(\mathfrak{a})$ at any principal ideal $\mathfrak{a} = (\alpha)$ with $\alpha \in \mathbb{Q}(\zeta_{l^n})$, $\alpha \equiv 1 \pmod{\pi_n}$ in terms of the Hilbert symbol. Note that when $l = 3$, they give the formula only for $r = 2$, but it is easy to derive our following formula for general r even if $l = 3$ from the case $r = 2$ in the same way as in the proof of Theorem 7.1 of [5], and note also that our formulation is slightly different from theirs, but they are essentially the same.

By Stickelberger's theorem on the prime ideal decomposition of Gauss sums, we have

$$J_{l^n}^{(a)}((\alpha)) = \zeta_{l^n}^{i(\alpha)}\alpha^{\omega_n(a)} \quad \text{with } i(\alpha) = i_{l^n}^{(a)}(\alpha) \in \mathbb{Z}/l^n\mathbb{Z}, \tag{$*$}$$

for any $\alpha \in \mathbb{Q}(\zeta_{l^n})$ such that $\alpha \equiv 1 \pmod{\pi_n}$, where

$$\omega_n(a) = \sum_{\substack{0<t<l^n \\ (t,l)=1}} \left(\sum_{i=0}^{r} \left\{\frac{a_i t}{l^n}\right\}\right)\sigma_{-t}^{-1} - \sum_{\substack{0<t<l^n \\ (t,l)=1}} \sigma_t \in \mathbb{Z}[G_n]$$

(cf. Weil [23]). Here $a_0 = -\Sigma_{i=1}^{r} a_i$, $G_n = \mathrm{Gal}(\mathbb{Q}_l(\zeta_{l^n})/\mathbb{Q}_l)$ and $\sigma_t \in G_n$ is such that $\zeta_{l^n}^{\sigma_t} = \zeta_{l^n}^t$.

THEOREM 3. *Let the notation and assumptions be as above. Assume that* $a = (a_1, \ldots, a_r) \not\equiv (0, \ldots, 0) \pmod{l^n}$. *Then*

$$\begin{aligned} i_{l^n}^{(a)}(\alpha) &\equiv g[l, \alpha]_n + h[1 + l, \alpha]_n \pmod{l^n} \\ &\equiv \left[\left(\prod_{i=0}^{r} a_i^{a_i}\right)(1 + l)^{T_1 + T_2}, \alpha\right]_n \pmod{l^n} \\ &\equiv \left[\left(\prod_{i=0}^{r} a_i^{a_i}\right)(1 + (T_1 + T_2)l), \alpha\right]_n \pmod{l^n} \end{aligned}$$

for $\alpha \in \mathbb{Q}(\zeta_{l^n})$, $\alpha \equiv 1 \pmod{\pi_n}$, *where*

$$g = \sum_{i=0}^{r} \mathrm{ord}_l(a_i) \cdot a_i,$$

$$h = cS_{l^n}^{(a)} \left(\equiv \left[\log \left(\prod_{i=0}^{r} a_i^{a_i} \right) \right] \Big/ \log(1+l) + T_1 + T_2 \pmod{l^n} \right),$$

$$c = \left(\left(1 - \frac{1}{l} \right) \log(1+l) \right)^{-1},$$

$$S_{l^n}^{(a)} = \sum_{\substack{0<t<l^n \\ (t,l)=1}} \left(\sum_{i=0}^{r} \left\{ \frac{a_i t}{l^n} \right\} \right) (-t)^{-1} (\in \mathbb{Z}_l),$$

$$T_1 = \frac{1}{l} \sum_{\substack{\mathrm{ord}_l(a_i)=n \\ 0 \leqslant i \leqslant r}} a_i,$$

and

$$T_2 = \begin{cases} \displaystyle\sum_{\substack{\mathrm{ord}_l(a_i)=n-1 \\ 0 \leqslant i \leqslant r}} a_i & \text{if } l = 3 \text{ and } n \geqslant 2, \\ 0 & \text{otherwise.} \end{cases}$$

Here $\mathrm{ord}_l(0) \cdot 0 = \infty \cdot 0 = 0$ *and* $0^0 = 1$.

Proof. Taking $\delta^{(n)}$ for $K = \mathbb{Q}_l$ (or for any K) of both members of the above (*) and using the properties (i) and (ii) in Lemma 1, we have

$$\delta^{(n)}(J_{l^n}^{(a)}((\alpha))) \equiv i_{l^n}^{(a)}(\alpha) + S_{l^n}^{(a)} \delta^{(n)}(\alpha) \pmod{l^n}.$$

Hence by (iii) of Lemma 1 and Theorem 1, we have

$$g\langle l, \alpha \rangle \equiv i_{l^n}^{(a)}(\alpha) - cS_{l^n}^{(a)}[1+l, \alpha]_n \pmod{l^n}.$$

Since $\langle l, \alpha \rangle = [l, \alpha]_n$ by class field theory, we have the first congruence. (Note that we use only Lemma 1 and Theorem 1 to obtain the first congruence). Now we use Corollary to Theorem 2 to transform the first congruence to the second one. By Corollary to Theorem 2 and the first congruence,

$$\begin{aligned} i_{l^n}^{(a)}(\alpha) &\equiv [l^g, \alpha]_n + c \left(\left(1 - \frac{1}{l} \right) \log \left(\prod_{i=0}^{r} \langle a_i \rangle^{a_i} \right) - T_1 - T_2 \right) [1+l, \alpha]_n \pmod{l^n} \\ &\equiv [l^g, \alpha]_n + [(1+l)^{h'}, \alpha]_n - c(T_1 + T_2)[1+l, \alpha]_n \pmod{l^n}, \end{aligned}$$

where

$$h' = \log\left(\prod_{i=0}^{r} \langle a_i \rangle^{a_i}\right) \Big/ \log(1 + l).$$

Since

$$(1 + l)^{h'} = \prod_{i=0}^{r} \langle a_i \rangle^{a_i},$$

$$c \equiv -1 \pmod{l},$$

and

$$T_1 + T_2 \equiv 0 \pmod{l^{n-1}},$$

we have

$$i_{l^n}^{(a)}(\alpha) \equiv \left[\prod_{i=0}^{r} (l^{\operatorname{ord}_l(a_i)} \langle a_i \rangle)^{a_i}, \alpha\right]_n + (T_1 + T_2)[1 + l, \alpha]_n \pmod{l^n}.$$

Since we can write

$$a_i^{a_i} = (\omega(a_i)\langle a_i \rangle l^{\operatorname{ord}_l(a_i)})^{a_i} \quad \text{for } 0 \leqslant i \leqslant r$$

$(\omega(a_i)^{l-1} = 1$, $\omega(0) = \langle 0 \rangle = 1$, and $l^{\infty} = 0)$ and since

$$\left[\prod_{i=0}^{r} \omega(a_i)^{a_i}, \alpha\right]_n \equiv 0 \pmod{l^n},$$

we have the second congruence. The last one follows directly from the second one, since $(1 + l)^{T_i} \equiv 1 + T_i l \pmod{l^{n+1}}$ and since $x \equiv 1 \pmod{l^{n+1}}$ implies $x \in (1 + l\mathbb{Z}_l)^{l^n}$ for $x \in \mathbb{Z}_l$.

If c is the minimum integer $c \geqslant 0$ such that

$$J_{l^n}^{(a)}((\alpha)) = \alpha^{\omega_n(a)} \qquad (*)$$

for all $\alpha \in \mathbb{Q}(\zeta_{l^n})$, $\alpha \equiv 1 \pmod{\pi_n^c}$, then we call the ideal (π_n^c) the *conductor* of the Jacobi sum Hecke character $J_{l^n}^{(a)}(\mathfrak{a})$, which we denote by $C_{l^n}^{(a)}$. Note that $c = 0$ if and only if the above $(*)$ holds for all $\alpha \in \mathbb{Q}(\zeta_{l^n})$ which are prime to l.

By the above Theorem 3, Lemma 8 below, and Coleman-McCallum's determination of the conductor $f_n(g, h)$ of the character $\alpha \mapsto [\alpha, l^g(1 + l)^h]_n$ with

$g \in \mathbb{Z}$, $h \in \mathbb{Z}_l$ ([5], Theorem 6.1) (note that we can also determine $f_n(g, h)$ by developing a certain computation in Iwasawa [8] (see Miki [18]), though Coleman-McCallum used Coleman's formula on the Hilbert norm residue symbol), we can get the precise conductor $C_{l^n}^{(a)}$ as follows:

COROLLARY

$$C_{l^n}^{(a)} = \begin{cases} (\pi_j \pi_{j+1}) & \textit{if } 1 \leqslant j \leqslant n-1 \quad \textit{and } \operatorname{ord}_l(g+hl) > j, \\ & \textit{otherwise}: \\ (\pi_j^2) & \textit{if } 1 \leqslant j \leqslant n-1 \quad \textit{or } n = \operatorname{ord}_l(h) + 1 \leqslant \operatorname{ord}_l(g), \\ (\pi_n) & \textit{if } j \geqslant n+1 \quad \textit{or } n = \operatorname{ord}_l(g) \leqslant \operatorname{ord}_l(h) \\ & \textit{and if } r_1 \textit{ is odd}, \\ (1) & \textit{if } j \geqslant n+1 \quad \textit{or } n = \operatorname{ord}_l(g) \leqslant \operatorname{ord}_l(h) \\ & \textit{and if } r_1 \textit{ is even}, \end{cases}$$

where $j = \min(\operatorname{ord}_l(g), \operatorname{ord}_l(h) + 1)$ *and* r_1 *is the number of* i *such that* $l^n \nmid a_i$ *for* $0 \leqslant i \leqslant r$.

Note that we have always $l \mid g$, since each term in g is 0 or 0 mod l according as $l \nmid a_i$ or not.

LEMMA 8. *Let the notation and assumptions be as in the above corollary. Furthermore, assume that*

$$J_{l^n}^{(a)}((\alpha)) = \alpha^{\omega_n(a)} \tag{$*$}$$

for all $\alpha \in \mathbb{Q}(\zeta_{l^n})$ *such that* $\alpha \equiv 1 \pmod{\pi_n}$. *Then* $C_{l^n}^{(a)} = (\pi_n)$ *or* (1) *according as* r_1 *is odd or even.*

Proof. For all $\alpha \in \mathbb{Q}(\zeta_{l^n})$ such that $(\alpha, l) = 1$, we can write

$$J_{l^n}^{(a)}((\alpha)) = \mathscr{E}(\alpha)\alpha^{\omega(a)}, \; \mathscr{E}(\alpha)^{2l^n} = 1 \tag{1}$$

(cf. Weil [23]). Since we can write

we have $\mathscr{E}(\alpha) = \alpha = \alpha_0\alpha_1$, $\alpha_0 \in \mathbb{Z}$, $1 \leqslant \alpha_0 \leqslant l-1$, $\alpha_1 \in \mathbb{Q}(\zeta_{l^n})^{\times}$, $\alpha_1 \equiv 1 \pmod{\pi_n}$, $\mathscr{E}(\alpha_1) = \mathscr{E}(\alpha_0)$ by the above ($*$). Since $\alpha_0^{l-1} \equiv 1 \pmod{l}$, by ($*$) we have $\mathscr{E}(\alpha_0^{l-1}) = \mathscr{E}(\alpha_0)^{l-1} = 1$. On the other hand, by (1) we have $\mathscr{E}(\alpha_0)^{2l^n} = 1$. Hence $\mathscr{E}(\alpha_0) = \pm 1$. Since $J_{l^n}^{(a)}((\alpha_0)) \equiv 1 \pmod{\pi_n}$, by (1) we have

$$\mathscr{E}(\alpha_0) \equiv \alpha_0^{-\omega_n(a)} \pmod{\pi_n}. \tag{2}$$

Since $\alpha_0 \in \mathbb{Z}$, by the definition of $\omega_n(a)$ we have

$$\alpha_0^{-\omega_n(a)} = \alpha_0^{-S+l^{n-1}(l-1)}, \tag{3}$$

where

$$S = \sum_{t \in (\mathbb{Z}/l^n\mathbb{Z})^\times} \left(\sum_{i=0}^{r} \left\{ \frac{a_i t}{l^n} \right\} \right).$$

Now, if necessary, we change the numbers of a_i so that $l^n \nmid a_i$ for $0 \leqslant i < r_1$, and $l^n \mid a_i$ for $r_1 \leqslant i \leqslant r$. Then

$$\begin{aligned} S &= \sum_{t \in (\mathbb{Z}/l^n\mathbb{Z})^\times} \sum_{i=0}^{r_1-1} \left\{ \frac{a_i t}{l^n} \right\} \\ &= \sum_{t} \sum_{i=0}^{r_1-1} \left\{ \frac{-a_i t}{l^n} \right\}. \end{aligned}$$

Hence

$$\begin{aligned} 2S &= \sum_{t} \sum_{i=0}^{r_1-1} \left(\left\{ \frac{a_i t}{l^n} \right\} + \left\{ \frac{-a_i t}{l^n} \right\} \right) \\ &= l^{n-1}(l-1) r_1, \end{aligned}$$

since $\{x\} + \{-x\} = 1$ if $x \in \mathbb{Q} - \mathbb{Z}$. Hence

$$S = r_1 l^{n-1} \cdot \frac{l-1}{2}. \tag{4}$$

By (2), (3), and (4), we have

$$\mathscr{E}(\alpha_0) \equiv \alpha_0^{-r_1 \cdot (l-1)/2} \pmod{\pi_n}, \tag{5}$$

since $\alpha_0^{l^{n-1}} \equiv \alpha_0 \pmod{l}$. Since $\mathscr{E}(\alpha_0) = \pm 1$, $\mathscr{E}(\alpha_0) = 1$ if and only if $\mathscr{E}(\alpha_0) \equiv 1 \pmod{\pi_n}$. Hence by (5) we see that $\mathscr{E}(\alpha_0) = 1$ for all $\alpha_0 \in \mathbb{Z}$ such that $1 \leqslant \alpha_0 \leqslant l-1$ if and only if $r_1 \equiv 0 \pmod{2}$.

Acknowledgements

This work was done while I was staying at the Institute for Advanced Study, Princeton in 1987/88, and it was written up during my stay at the I.H.E.S.

(Institut des Hautes Etudes Scientifiques, Bures-sur-Yvette) in 1991/92. I wish to express my sincere gratitude to both Institutes for their hospitality. I wish to thank G. Anderson, P. Deligne, B. Dwork, S. Sperber, A. Weil, and A. Wiles for their encouragement while I was in Princeton. I also wish to thank G. Anderson, H. Cohn, R. Coleman, W. McCallum, and S. Sperber for valuable conversations while I was staying at the Graduate Center of CUNY (City University of New York), MSRI (Mathematical Sciences Research Institute, Berkeley), and the University of Minnesota. I also wish to thank T. Tamagama, H. Jacquet and D. Goldfeld for helpful discussions when I was invited to give talks at the Algebra Seminar in Yale University in January 1988 and at the Number Theory Seminar (Goldfeld) in Columbia University in March 1988. Finally, I wish to thank the Department of Mathematics, the Graduate Center of CUNY, MSRI, and the University of Minnesota for their hospitality.

References

1. Anderson, G.: The hyperadelic gamma function, *Invent. Math.* 95 (1989) 63–131.
2. Artin, ED., Hasse, H.: Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswureln, *Abh. Math. Sem. Univ. Hamburg* 6 (1928) 146–162.
3. Coates, J., Wiles, A.: Explicit reciprocity laws, *Astèrisque* 41/42 (1977) 7–17.
4. Coleman, R.: Anderson-Ihara theory: Gauss sums and circular units, *Advanced Studies in Pure Math.* 17 (1989) 55–72.
5. Coleman, R., McCallum, W.: Stable reduction of Fermat curves and Jacobi sum Hecke characters, *J. reine und angew. Math.* 385 (1988) 41–101.
6. Hasse, H.: *Zetafunktionen und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus.* Abh. Deut. Akad. Wiss. Berlin Kl. Math. Nat., 1954, no. 4 (1955) 70 pp.
7. Ihara, Y.: Profinite braid groups, Galois representations and complex multiplications, *Ann. of Math.* 123 (1986), 43–106.
8. Iwasawa, K.: On explicit formulas for the norm residue symbol, *J. Math. Soc. Japan* 20 (1968) 151–165.
9. Iwasawa, K: On p-adic L-functions, *Ann. of Math.* 89 (1969) 198–205.
10. Iwasawa, K.: Lectures on p-adic L-functions. Ann. of Math. Studies 74, Princeton University Press 1972.
11. Iwasawa, K.: A note on Jacobi sums, *Symposia Math.* 15 (1975) 447–459.
12. Jensen, C.: Über die Führer einer Klasse Heckescher Grössencharaktere, *Math. Scand.* 8 (1960) 81–96.
13. Kato, K.: A generalization of class field theory (Japanese). *Sûgaku* 40 (1988) 289–311.
14. Miki, H.: On the l-adic expansion of certain Gauss sums and its applications, *Advanced Studies in Pure Math.* 12 (1987) 87–118.
15. Miki, H.: On Weil's Grössencharacters: A brief survey of Gauss and Jacobi sums and recent developments. Proc. Symp. on Number Theory, Nagasaki, Japan, Nov. 1986.
16. Miki, H.: On the conductor of the Jacobi sum Hecke character. Preprint April 1988, 10 pp. (unpublished) = talk in Number Theory Seminar (Goldfeld), Columbia Univ., March 21, 1988.
17. Miki, H.: On the congruence for Gauss sums and its applications. In: *Thèorie des nombres – Number Theory,* J.-M. De Koninck, C. Levesque (eds.). Proceedings, Laval 1987, pp. 632–641. Walter de Gruyter: Berlin, New York, 1989.