Advanced Studies in Pure Mathematics 12, 1987
Galois Representations and Arithmetic Algebraic Geometry
pp. 87–118

On the l-Adic Expansion of Certain Gauss Sums and Its Applications*)

Hiroo Miki

Introduction

In the present paper, we shall give a new explicit formula on the l-adic expansion (mod π^l) of certain Gauss sums (see Theorem 1 in Section 1).

Let p be any prime number and let $m>1$ be a natural number which is not divisible by p. Let ζ_m be a primitive m-th root of unity in the field of complex numbers $\boldsymbol{C}$. Let $\boldsymbol{Q}$ be the field of rational numbers and let $\boldsymbol{Z}$ be the ring of rational integers. Fix a prime ideal $\mathfrak{p}$ of $\boldsymbol{Q}(\zeta_m)$ lying above p and put $N\mathfrak{p}=q$, where $N\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$. Note that $m|(q-1)$. Let $\boldsymbol{F}_q$ be the finite field of q elements. Let

$$\chi_{\mathfrak{p}}(x \bmod \mathfrak{p})=\left(\frac{x}{\mathfrak{p}}\right)_m$$

be the m-th power residue symbol in $\boldsymbol{Q}(\zeta_m)$, i.e.,

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

for $x \in \boldsymbol{Z}[\zeta_m]$. $\chi_{\mathfrak{p}}$ induces a homomorphism of the multiplicative group $\boldsymbol{F}_q^{\times}$ of $\boldsymbol{F}_q$ to $\boldsymbol{C}^{\times}$ of order m and $\chi_{\mathfrak{p}}(0)=0$. Here we identify $\boldsymbol{F}_q$ and $\boldsymbol{Z}[\zeta_m]/\mathfrak{p}$. Let T be the trace of $\boldsymbol{F}_q$ to $\boldsymbol{F}_p$ and put

$$\psi(x)=\zeta_p^{T(x)}$$

for $x \in \boldsymbol{F}_q$. Then ψ is a homomorphism of the additive group $\boldsymbol{F}_q$ to the multiplicative group $\boldsymbol{C}^{\times}$.

Definition. For each $a \in \boldsymbol{Z}$, put

Received May 29, 1986.

*) This is the details of my lecture in Symp. on Algebraic Number Theory, October 1985 at the Research Institute for Mathematical Sciences Kyoto Univ., which is a revised and extended version of my intensive lectures at Kanazawa Univ. and Tokyo Institute of Technology in Jan.-Feb. 1985. I also gave my intensive lecture related to this subject at Kyushu Univ. in Dec. 1985 and at Nagoya Univ. in July 1986.

$$g_m(\mathfrak{p}, a) = -\sum_{x \in \boldsymbol{F}_q} \chi_{\mathfrak{p}}^a(x)\psi(x).$$

This is called the *Gauss sum*. We write $g(\chi_{\mathfrak{p}}^a)$ or $g(a)$ for $g_m(\mathfrak{p}, a)$ if there is no confusion. Clearly $g(a) \in \boldsymbol{Q}(\zeta_{mp})$.

The purpose of the present paper is to give a partial answer to the following question:

(*) To give an explicit formula on the π-adic expansion of $g(\chi_{\mathfrak{p}}^a)$ when m is a power of a prime number l, taking a suitable prime element π of $\boldsymbol{Q}_l(\zeta_m)$.

Namely, we shall give an explicit formula on the π-adic expansion of $g(\chi_{\mathfrak{p}}^a) \pmod{\pi^l}$.

As its applications, we shall obtain the following (I)–(IV):

(I) *generalization of Iwasawa's congruences* [8] *and Ihara's congruences* [5] *on Jacobi sums.*

Iwasawa ([8], Theorem 1) gives the congruence for Jacobi sums to determine the conductor of Jacobi sum Hecke characters in $\boldsymbol{Q}(\zeta_l)$, and Ihara ([5], Corollary to Theorem 7) gives a generalization of Iwasawa's formula to the l-power case, by using his "universal" power series for Jacobi sums. In Theorem 2 in Section 2, we shall give a generalization of Iwasawa's congruence and Ihara's congruence, by using Theorem 1 in Section 1 and a well known relation between Jacobi sums and Gauss sums (see also Lemma 4 in Section 2). In Section 2, we shall also give another proof of Theorem 1 using Uehara's method of computation on Jacobi sums (see the proof of Lemma 1 in [11]). In Section 5, we shall give another proof of Theorem 1 when $n=1$, by using Iwasawa's formula on power residue symbol for cyclotomic units ([9], Lemma 1). After the Kyoto conference in Oct. 1985, Anderson [1] obtained another proof of our Theorems 1 and 2 (see Section 2, *Note*). Thus we have four different proofs of our Theorems 1 and 2, and we note that our original proof of Theorems 1 and 2 is the most elementary one.

Our first motivation of our problem was to give an algebraic proof of the nonvanishing of certain character sums. As is stated in (II) below, Iwasawa [9] gives an algebraic proof of $\sum_{a=1}^{l-1} a\delta(a) \neq 0$ for an odd Dirichlet character δ of conductor l under a certain condition. In June 1984, we obtained another algebraic proof of $\sum_{a=1}^{l-1} a\delta(a) \neq 0$ in the same case as Iwasawa's, using the l-adic expansion of Gauss sums (slightly weaker, but essentially the same as the formula in Theorem 1 in Section 1). Our method of proof of Theorem 1 can be regarded as a generalization of the proof of Iwasawa's congruence [8], Theorem 1.

On the other hand, there is a series of interesting works Ihara [5], Coleman [2], Ihara-Kaneko-Yukinari [6] and Anderson [1] on the universal

power series for Jacobi sums and Gauss sums, which are closely related to our problem of the l-adic expansion of Gauss sums. Although the present work was done independently, the mutual relationship became clear gradually, and at last Coleman and Anderson [1] obtained another proof of our Theorems 1 and 2 as is stated as above (see *Note* at the end of Section 2).

(II) *algebraic proof of the nonvanishing of the character sum* $\sum_{b=1}^{m} b\delta(b)$ *in certain cases, where* δ *is a primitive odd Dirichlet character of conductor* m.

Put $M(\delta)=\sum_{b=1}^{m} b\delta(b)$. The only proof of $M(\delta)\neq 0$ in the general case follows from the fact that the value $L(1, \delta)$ of Dirichlet L function $L(s, \delta)$ at $s=1$ is non-zero, and *algebraic* proofs are known only in the following three cases (i)–(iii):

(i) $m=l^n$ (l is a prime number and $n\geqq 1$) and δ is faithful, i.e., $\mathrm{Ker}\,\delta=\{1\}$ (see Hasse [4], pp. 90–94 and Ullom [12]).

(ii) $m=l^n$ (l is a prime number and $n\geqq 1$) and the order of δ is 2^t with $t\geqq 1$ (see Hasse [4], pp. 90–94, Ullom [12] and Metsänkylä [10]).

(iii) $m=l$ ($l\geqq 5$ is a prime number) and $\varepsilon_{\omega\delta^{-1}}\notin \boldsymbol{Q}(\zeta_l)^l$ (Iwasawa [9]) (For $\varepsilon_{\omega\delta^{-1}}$, see Section 1).

An algebraic proof in the case (iii) follows directly from a highly interesting explicit formula of Iwasawa on the l-th power residue symbol for cyclotomic units ([9], Lemma 1).

In Section 3, we shall give an elementary algebraic proof of $M(\delta)\neq 0$ in the case (iii) as an application of Theorem 1. In fact, we shall give an algebraic proof of $M(\delta)\neq 0$ in the following case (iii)′ which generalizes (iii).

(iii)′ $m=l^n$ ($l\geqq 5$ is a prime number and $n\geqq 1$) and $\varepsilon_{\omega\delta_1^{-1}}\notin \boldsymbol{Q}(\zeta_l)^l$ (see Section 3.3).

We shall also show that the above cases (i) and (ii) can be proved algebraically by using Gauss sums. Namely, we can deal with all known cases uniformly by using Gauss sums to some extent.

(III) *Another proof of a necessary and sufficient condition for* $\varepsilon_\phi\in \boldsymbol{Q}(\zeta_l)^l$ *due to Iwasawa* [9].

Iwasawa's proof is essentially based on Artin-Hasse's explicit formula on the norm residue symbol in local class field theory, and Uehara [11] gives another proof of this result of Iwasawa by using Jacobi sums. In Section 4, we shall give another proof of this result of Iwasawa by using Theorem 1 and Stickelberger's theorem.

(IV) *Another elementary proof of Iwasawa's formula on the l-th power residue symbol for cyclotomic units in* $\boldsymbol{Q}(\zeta_l)$ *(Iwasawa* [9]).

Iwasawa [9], Lemma 1 gives a highly interesting explicit formula on the l-th power residue symbol for cyclotomic units in $\boldsymbol{Q}(\zeta_l)$, by using Artin-Hasse's explicit formula on the norm residue symbol in local class

field theory.

In Section 5, we shall give an elementary proof of Iwasawa's formula by using Theorem 1. Conversely, we can prove Theorem 1 when $n=1$, by using Iwasawa's formula. The link between Iwasawa's formula and our Theorem 1 is essentially Stickelberger's theorem (see Lemma 12 in Section 5).

Acknowledgement. I wish to express my sincere gratitude to Prof. K. Iwasawa for valuable conversations during his stay in Japan in July 1984, and to Prof. Y. Ihara for his interesting lectures at Tokyo Metropolitan University in Dec. 1984 and for stimulating discussions. I also wish to thank Prof. G. W. Anderson for stimulating discussions during the Kyoto Symposium in Oct. 1985. Finally, I wish to thank the Departments of Mathematics, Kanazawa University, Tokyo Institute of Technology, Kyushu University and Nagoya University for giving me chances to give lectures related to this subject, and for their hospitality.

§ 1. Congruence for Gauss sums

In this section, let $m=l^n$ be a power of any prime number l with $n\geqq 1$. Let $\boldsymbol{Z}_l$ be the ring of l-adic integers. Let $\bar{\boldsymbol{Q}}$ be the algebraic closure of $\boldsymbol{Q}$ in $\boldsymbol{C}$ and let $\bar{\boldsymbol{Q}}_l$ be a fixed algebraic closure of the field of l-adic numbers $\boldsymbol{Q}_l$. Fix a primitive l^i-th root of unity ζ_{l^i} such that $\zeta_{l^{i+1}}^l=\zeta_{l^i}$ for $i\geqq 1$.

By a fixed imbedding $\bar{\boldsymbol{Q}}\subset\bar{\boldsymbol{Q}}_l$, we consider $\bar{\boldsymbol{Q}}$ as a subfield of $\bar{\boldsymbol{Q}}_l$. Let $\pi\in\boldsymbol{Q}_l(\zeta_{l^n})$ be such that

$$\pi\equiv \operatorname{Log}\zeta_{l^n} \qquad (\operatorname{mod}(\zeta_{l^n}-1)^l),$$

where $\operatorname{Log}X=\sum_{i=1}^{l-1}(-1)^{i-1}(X-1)^i/i\in\boldsymbol{Z}_l[X]$. Then π is a prime element of $\boldsymbol{Q}_l(\zeta_{l^n})$ and we have

$$\zeta_{l^n}\equiv \operatorname{Exp}\pi \qquad (\operatorname{mod}\pi^l),$$

where

$$\operatorname{Exp}X=\sum_{i=0}^{l-1}\frac{X^i}{i!}\in\boldsymbol{Z}_l[X].$$

For any ideal $\mathfrak{a}$ of $\boldsymbol{Q}(\zeta_{l^n})$ which is prime to l and for any $x\in\boldsymbol{Q}(\zeta_{l^n})$ which is prime to $\mathfrak{a}$, let $(x/\mathfrak{a})_{l^s}$ be the l^s-th power residue symbol in $\boldsymbol{Q}(\zeta_{l^n})$ and let $[x,\mathfrak{a}]_{l^s}\in\boldsymbol{Z}/l^s$ be such that

$$\left(\frac{x}{\mathfrak{a}}\right)_{l^s}=\zeta_{l^s}^{[x,\mathfrak{a}]_{l^s}} \qquad (1\leqq s\leqq n).$$

Then we have

$$[x, \mathfrak{a}]_l \equiv [x, \mathfrak{a}]_{l^s} \pmod{l},$$

for $1 \leqq s \leqq n$. Put

$$\lambda_{\mathfrak{p}}^{(s)}(x \bmod \mathfrak{p}) = \begin{cases} [x, \mathfrak{p}]_{l^s} & \text{if } (x, \mathfrak{p}) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathfrak{p}$ is as in the introduction.

Then $\lambda_{\mathfrak{p}}^{(s)}$ induces a surjective homomorphism of the multiplicative group $\boldsymbol{F}_q^\times$ to the additive group $\boldsymbol{Z}/l^s$. For simplicity, put $\lambda = \lambda_{\mathfrak{p}} = \lambda_{\mathfrak{p}}^{(1)}$.

Now we shall state the definition of cyclotomic units in $\boldsymbol{Q}(\zeta_l)$. We identify the Galois group $G = \mathrm{Gal}(\boldsymbol{Q}(\zeta_l)/\boldsymbol{Q})$ and $\boldsymbol{F}_l^\times = (\boldsymbol{Z}/l)^\times$ by the correspondence $\sigma_b \leftrightarrow b \bmod l\boldsymbol{Z}$ with $b \in \boldsymbol{Z}$, where $\sigma_b(\zeta_l) = \zeta_l^b$. Hence we have $\phi(\sigma_b) = \phi(b)$ and $\phi(b) \in \boldsymbol{Z}[\zeta_{l-1}] \subset \boldsymbol{Z}_l$ for $b \in \boldsymbol{F}_l$ and $\phi \in \hat{G}$ ($\hat{G}$ is the character group of G). For each $\phi \in \hat{G}$, put

$$e_\phi = \frac{1}{l-1} \sum_{d=1}^{l-1} \phi^{-1}(d)\sigma_d \in \boldsymbol{Z}_l[G],$$

where $\boldsymbol{Z}_l[G]$ is the group ring of G over $\boldsymbol{Z}_l$. Let $\omega \in \hat{G}$ be the Teichmüller character, i.e., the character satisfying

$$\omega(d) \equiv d \pmod{l\boldsymbol{Z}_l}$$

for $d \in \boldsymbol{Z}$. If $l \geqq 5$ and if $\phi = \omega^{-2i}$ with $1 \leqq i \leqq (l-3)/2$, then there exists

$$\mu = \sum_{d=1}^{l-1} m_d \sigma_d \in \boldsymbol{Z}[G]$$

with $m_d \in \boldsymbol{Z}$ satisfying

$$\sum_{d=1}^{l-1} m_d = 0 \quad \text{and} \quad \mu \equiv e_\phi \pmod{l\boldsymbol{Z}_l[G]}.$$

Definition. If $l \geqq 5$, then put

$$\varepsilon_\phi = \varepsilon_{2i} = (1-\zeta_l)^\mu = \prod_{d=1}^{l-1} (1-\zeta_l^d)^{m_d}$$

for $1 \leqq i \leqq (l-3)/2$. We call ε_ϕ the *cyclotomic unit* in $\boldsymbol{Q}(\zeta_l)$.

Under the above notation and assumptions, we have the following

Theorem 1. *Let l be any prime number and assume that $m=l^n$ with $n\geqq 1$. Then for each $a\in \boldsymbol{Z}$, we have*

$$g(\chi_{\mathfrak{p}}^{a})\equiv \mathrm{Exp}\,(\alpha_1(a\pi)+\sum_{i=1}^{(l-3)/2}\beta_{2i}\frac{(a\pi)^{2i+1}}{(2i+1)!}+\frac{q-1}{2l}(a\pi)^{l-1}) \qquad (\mathrm{mod}\ \pi^l),$$

where $\alpha_1=-\sum_{x\in \boldsymbol{F}_q^{\times}}\lambda(x)\psi(x)$ and $\beta_{2i}=-[\varepsilon_{2i},\mathfrak{p}]_l$ with $1\leqq i\leqq(l-3/2)$. Here we omit the term $\sum_{i=1}^{(l-3)/2}$ if $l\leqq 3$, and omit the term $((q-1)/2l)(a\pi)^{l-1}$ if $l=2$.

Remark. (1) We define the product $\bar{x}y\ (\mathrm{mod}\ \pi^l)$ of $\bar{x}\in \boldsymbol{F}_l(\bar{\zeta}_p)$ ($\bar{\zeta}_p=\zeta_p \bmod l\boldsymbol{Z}_l[\zeta_p]$) and $y\in \pi\boldsymbol{Z}_l[\zeta_{p^n}]$ as the product $xy \bmod \pi^l$, where $x\in \boldsymbol{Z}_l[\zeta_p]$ is such that $x \bmod l=\bar{x}$. It is well defined, since $\mathrm{ord}_{\pi}\,(l)=(l-1)l^{n-1}$, where ord_{π} is the normalized additive valuation of $\boldsymbol{Q}_l(\zeta_{l^n})$.

(2) In the definition of α_1, we write $\psi(x)$ for $\psi(x) \bmod l\boldsymbol{Z}_l[\zeta_p]$ for simplicity.

For the proof of the above theorem, we need the following Lemmas 1, 2 and 3.

Lemma 1. *For $0\leqq j\leqq l-1$, we have*

$$\sum_{b\in \boldsymbol{F}_q^{\times}-\{1\}}\lambda(b)^j=\begin{cases}-1 & \text{if } j=0,\\ 0 & \text{if } 1\leqq j\leqq l-2,\\ -\dfrac{q-1}{l} & \text{if } j=l-1,\end{cases}$$

where $\lambda(b)^0=1$.

Proof. If $j=0$, then

$$\sum_{b\in \boldsymbol{F}_q^{\times}-\{1\}}\lambda(b)^j=(q-1)-1=-1,$$

since $q-1\equiv 0\,(\mathrm{mod}\ l)$. Now assume that $1\leqq j\leqq l-1$. Since λ is a surjective homomorphism of $\boldsymbol{F}_q^{\times}$ onto $\boldsymbol{F}_l$, this induces the isomorphism

$$\boldsymbol{F}_q^{\times}/(\boldsymbol{F}_q^{\times})^l\simeq \boldsymbol{F}_l.$$

Hence λ takes a constant value on each class of $\boldsymbol{F}_q^{\times}/(\boldsymbol{F}_q^{\times})^l$. Let R be a complete representative system of $\boldsymbol{F}_q^{\times}/(\boldsymbol{F}_q^{\times})^l$. Then

$$\sum_{b\in \boldsymbol{F}_q^{\times}}\lambda(b)^j=|(\boldsymbol{F}_q^{\times})^l|\sum_{b\in R}\lambda(b)^j$$

$$=\frac{q-1}{l}\sum_{m=1}^{l-1} m^j,$$

where $|(\boldsymbol{F}_q^\times)^l|$ is the number of elements in $(\boldsymbol{F}_q^\times)^l$. Let f_j be the homomorphism of $\boldsymbol{F}_l^\times$ to $\boldsymbol{F}_l^\times$ defined by $f_j(x)=x^j$. Then $f_j=1$ or not according as $j=l-1$ or $1\leqq j\leqq l-2$, so we have

$$\sum_{m=1}^{l-1} m^j=\sum_{m\in \boldsymbol{F}_l^\times} f_j(m)=\begin{cases} 0 & \text{if } 1\leqq j\leqq l-2,\\ -1 & \text{if } j=l-1.\end{cases}$$

Thus we have the assertion.

Lemma 2. *Assume* $l\geqq 5$. *For* $0\leqq i\leqq l-2$, *put*

$$\beta_i=\sum_{b\in \boldsymbol{F}_q} \lambda(b)^i\lambda(1-b).$$

Then

$$\beta_i=\begin{cases} 0 & \text{if } i=0 \text{ or if } i(1\leqq i\leqq l-4) \text{ is odd},\\ -\dfrac{q-1}{2l} & \text{if } i=l-2.\end{cases}$$

Proof. Since

$$\beta_0=\sum_{b\in \boldsymbol{F}_q} \lambda(b),$$

so $\beta_0=0$ by Lemma 1. Now assume that i is odd and $1\leqq i\leqq l-2$. Then

$$\begin{aligned}\beta_i&=\sum_{b\in \boldsymbol{F}_q^\times} \lambda(b)^i\lambda(1-b)\\ &=\sum_{b\in \boldsymbol{F}_q^\times} \lambda(b^{-1})^i\lambda(1-b^{-1}).\end{aligned}$$

Hence

$$\begin{aligned}\beta_i&=\sum_{b\in \boldsymbol{F}_q^\times} (-\lambda(b))^i\lambda(b^{-1}(b-1))\\ &=-\sum_{b\in \boldsymbol{F}_q^\times-\{1\}} \lambda(b)^i(-\lambda(b)+\lambda(b-1))\end{aligned}$$

since i is odd. Hence

$$\begin{aligned}\beta_i&=\sum_{b\in \boldsymbol{F}_q^\times-\{1\}} \lambda(b)^{i+1}-\sum_{b\in \boldsymbol{F}_q^\times-\{1\}} \lambda(b)^i\lambda((-1)(1-b))\\ &=\sum_{b\in \boldsymbol{F}_q^\times-\{1\}} \lambda(b)^{i+1}-\beta_i,\end{aligned}$$

since $\lambda((-1)(1-b))=\lambda(1-b)$. Hence

$$\beta_i=\frac{1}{2}\sum_{b\in \boldsymbol{F}_q^\times-\{1\}}\lambda(b)^{i+1},$$

so we have the assertion by Lemma 1.

Lemma 3. *Assume $l\geqq 5$. Then for $1\leqq i\leqq(l-3)/2$, we have*

$$\beta_{2i}=-\lambda(\varepsilon_{2i} \bmod \mathfrak{p}).$$

In particular, $\beta_{2i}=0$ if and only if $\varepsilon_{2i} \bmod \mathfrak{p}\in(\boldsymbol{F}_q^\times)^l$.

Proof. Since λ induces the isomorphism $\boldsymbol{F}_q^\times/(\boldsymbol{F}_q^\times)^l\simeq \boldsymbol{F}_l$, λ takes a constant value on each class of $\boldsymbol{F}_q^\times/(\boldsymbol{F}_q^\times)^l$. Let R ($\ni 1$) be a complete representative system of $\boldsymbol{F}_q^\times/(\boldsymbol{F}_q^\times)^l$. Then

$$\begin{aligned}\beta_{2i}&=\sum_{b\in \boldsymbol{F}_q^\times}\lambda(b)^{2i}\lambda(1-b)\\&=\sum_{b\in R}\sum_{c\in(\boldsymbol{F}_q^\times)^l}\lambda(bc)^{2i}\lambda(1-bc)\\&=\sum_{b\in R}\lambda(b)^{2i}\sum_{c\in(\boldsymbol{F}_q^\times)^l}\lambda(1-bc)\\&=\sum_{b\in R-\{1\}}\lambda(b)^{2i}\lambda\Big(\prod_{c\in(\boldsymbol{F}_q^\times)^l}(1-bc)\Big).\end{aligned}$$

Put $h=(q-1)/l$. Then $h\not\equiv 0 \pmod p$. Since $(\boldsymbol{F}_q^\times)^l$ is the group of h-th roots of unity in $\bar{\boldsymbol{F}}_p$ (an algebraic closure of $\boldsymbol{F}_p$), we have

$$\prod_{c\in(\boldsymbol{F}_q^\times)^l}(1-bc)=1-b^h.$$

So,

$$\beta_{2i}=\sum_{b\in R-\{1\}}\lambda(b)^{2i}\lambda(1-b^h).$$

Let l^t be the exact power of l dividing $(q-1)$, and let $\eta\in\boldsymbol{F}_q^\times$ be an element of order l^t with $\lambda(\eta)=1$. If we take the set $\{1,\eta,\eta^2,\cdots,\eta^{l^t-1}\}$ as R, then

$$\beta_{2i}=\sum_{d=1}^{l-1}d^{2i}\lambda(1-(\eta^h)^d).$$

If we put $\xi=\eta^h$, then

$$\beta_{2i}=\lambda\Big(\prod_{d=1}^{l-1}(1-\xi^d)^{d^{2i}}\Big). \tag{1}$$

Let $x \in \boldsymbol{Z}[\zeta_{l^n}]$ be such that $x \bmod \mathfrak{p} = \eta$. By the definition of $\chi_\mathfrak{p}$,

$$\chi_\mathfrak{p}(x \bmod \mathfrak{p}) \equiv x^{(q-1)/l^n} \pmod{\mathfrak{p}}.$$

On the other hand, by the definition of $\lambda_\mathfrak{p}^{(n)}$,

$$\chi_\mathfrak{p}(x \bmod \mathfrak{p}) = \zeta_{l^n}^{\lambda_\mathfrak{p}^{(n)}(\eta)}.$$

Taking the l^{n-1}-th power of the both members, we have

$$\chi_\mathfrak{p}(x \bmod \mathfrak{p})^{l^{n-1}} = \zeta_l^{\lambda(\eta)} = \zeta_l,$$

since $\lambda(\eta) \equiv \lambda_\mathfrak{p}^{(n)}(\eta) \pmod{l}$. Hence

$$\zeta_l \bmod \mathfrak{p} = \eta^{(q-1)/l},$$

so

$$\zeta_l \bmod \mathfrak{p} = \xi. \tag{2}$$

In the definition of ε_{2i},

$$\begin{aligned} m_a &\equiv -\omega^{2i}(d) && \pmod{l\boldsymbol{Z}_l} \\ &\equiv -d^{2i} && \pmod{l\boldsymbol{Z}}. \end{aligned}$$

Hence

$$\varepsilon_{2i} \equiv \left(\prod_{d=1}^{l-1} (1-\zeta_l^d)^{a^{2i}} \right)^{-1} \qquad \bmod (\boldsymbol{Q}(\zeta_l)^\times)^l,$$

so

$$(\varepsilon_{2i} \bmod \mathfrak{p}) \cdot \prod_{d=1}^{l-1} (1-\xi^d)^{a^{2i}} \in (\boldsymbol{F}_q^\times)^l$$

by (2). Hence we have

$$\beta_{2i} = -\lambda(\varepsilon_{2i} \bmod \mathfrak{p})$$

by (1).

Now we prove Theorem 1.

Proof of Theorem 1. By the definition of $\lambda_\mathfrak{p}^{(n)}$,

$$\begin{aligned} g(\chi_\mathfrak{p}^a) &= -\sum_{x \in \boldsymbol{F}_q^\times} \chi_\mathfrak{p}^a(x)\psi(x) \\ &\equiv -\sum_{x \in \boldsymbol{F}_q^\times} (\operatorname{Exp} \pi)^{\lambda_\mathfrak{p}^{(n)}(x)a} \psi(x) \qquad \pmod{\pi^l}. \end{aligned}$$

Since $(\mathrm{Exp}\,\pi)^l \equiv 1 \pmod{\pi^l}$ and $\lambda(x) \equiv \lambda_{\mathfrak{p}}^{(n)}(x) \pmod{l}$, we have

$$g(\chi_{\mathfrak{p}}^a) \equiv -\sum_{x \in \boldsymbol{F}_q^\times} (\mathrm{Exp}\,(\lambda(x)a\pi))\psi(x) \qquad (\mathrm{mod}\ \pi^l)$$

$$\equiv 1 + \sum_{i=1}^{l-1} \left(-\sum_{x \in \boldsymbol{F}_q^\times} \lambda(x)^i \psi(x)\right) \frac{(a\pi)^i}{i!} \qquad (\mathrm{mod}\ \pi^l),$$

since $\sum_{x \in \boldsymbol{F}_q} \psi(x) = 0$. Put

$$\alpha_i = -\sum_{x \in \boldsymbol{F}_q^\times} \lambda(x)^i \psi(x)$$

for $0 \leqq i \leqq l-1$ (since $\lambda(x)^0 = 1$, we have $\alpha_0 = 1$). Then

$$g(\chi_{\mathfrak{p}}^a) \equiv 1 + \sum_{i=1}^{l-1} \alpha_i \frac{(a\pi)^i}{i!} \qquad (\mathrm{mod}\ \pi^l). \tag{1}$$

Assume that $1 \leqq i \leqq l-3$. By the definition of α_i, we have

$$\alpha_i \alpha_1 = \left(\sum_{b \in \boldsymbol{F}_q} \lambda(b)^i \psi(b)\right)\left(\sum_{c \in \boldsymbol{F}_q} \lambda(c)\psi(c)\right)$$

$$= \sum_{b, d \in \boldsymbol{F}_q} \lambda(b)^i \lambda(d-b)\psi(d).$$

In the summation $\sum_{b, d \in \boldsymbol{F}_q}$, we divide the case $d = 0$ and $d \neq 0$. Then

$$\alpha_i \alpha_1 = \sum_{b \in \boldsymbol{F}_q} \lambda(b)^{i+1} + \sum_{d \in \boldsymbol{F}_q^\times} \left(\sum_{b \in \boldsymbol{F}_q} \lambda(b)^i \lambda(d-b)\right)\psi(d)$$

since $\lambda(-b) = \lambda(b)$. Hence by Lemma 1,

$$\alpha_i \alpha_1 = \sum_{d \in \boldsymbol{F}_q^\times} \left(\sum_{b \in \boldsymbol{F}_q} \lambda(b)^i \lambda(d-b)\right)\psi(d),$$

since $2 \leqq i+1 \leqq l-2$. Put

$$A_d = \sum_{b \in \boldsymbol{F}_q} \lambda(b)^i \lambda(d-b)$$

with $d \in \boldsymbol{F}_q^\times$. Then

$$\alpha_i \alpha_1 = \sum_{d \in \boldsymbol{F}_q^\times} A_d \psi(d). \tag{2}$$

Next, we compute A_d. By replacing b by db,

$$A_d = \sum_{b \in \boldsymbol{F}_q^\times} \lambda(db)^i \lambda(d-db),$$

so

$$A_d=\sum_{b\in \boldsymbol{F}_q^\times-\{1\}}\left(\sum_{j=0}^{i}\binom{i}{j}\lambda(d)^{i-j}\lambda(b)^j\right)(\lambda(d)+\lambda(1-b)),$$

since $\lambda(db)=\lambda(d)+\lambda(b)$. Hence

$$A_d=-\lambda(d)^{i+1}+\sum_{j=1}^{i}\binom{i}{j}\lambda(d)^{i-j}\beta_j$$

by Lemma 1 and since $\beta_0=0$ by Lemma 2. Hence by (2), we have

$$\alpha_i\alpha_1=\alpha_{i+1}-\sum_{j=1}^{i}\binom{i}{j}\alpha_{i-j}\beta_j \qquad \text{for } 0\leqq i\leqq l-3. \tag{3}$$

If $i=l-2$, then in the same way as above, we have

$$\alpha_{i+1}=\alpha_i\alpha_1+\sum_{j=1}^{i-1}\binom{i}{j}\alpha_{i-j}\beta_j-\beta_i \qquad \text{for } i=l-2. \tag{4}$$

Thus by (3) and (4), we have

$$\alpha_{i+1}=\sum_{j=0}^{i}\binom{i}{j}\alpha_{i-j}\gamma_j \qquad \text{for } 0\leqq i\leqq l-2, \tag{5}$$

where

$$\gamma_i=\begin{cases}\alpha_1 & \text{if } i=0,\\ \beta_i & \text{if } 1\leqq i\leqq l-3,\\ -\beta_i & \text{if } i=l-2.\end{cases}$$

Now assume that

$$\sum_{i=0}^{l-1}\alpha_i\frac{X^i}{i!}\equiv \operatorname{Exp} f(X) \pmod{X^l}, \tag{6}$$

where

$$f(X)=\sum_{i=1}^{l-1}\lambda_i\frac{X^i}{i!}\in \boldsymbol{F}_l(\bar{\zeta}_p)[X].$$

Put $F(X)=\operatorname{Exp} f(X)$. Then

$$F'(X)\equiv F(X)f'(X) \pmod{X^{l-1}}.$$

By differentiating the both members i times ($0\leqq i\leqq l-2$), we have

$$F^{(i+1)}(X)\equiv\sum_{j=0}^{i}\binom{i}{j}F^{(i-j)}(X)f^{(j+1)}(X) \qquad (\mathrm{mod}\ X).$$

Put $X=0$. Then by (6) we have

$$\alpha_{i+1}=\sum_{j=0}^{i}\binom{i}{j}\alpha_{i-j}\lambda_{j+1} \tag{7}$$

for $0\leqq i\leqq l-2$. In particular, $\alpha_1=\lambda_1$, so $\lambda_1=\gamma_0$. Hence by (5) and (7), we have

$$\lambda_{j+1}=\gamma_j \tag{8}$$

for $0\leqq j\leqq l-2$. Conversely, (8) implies (6). If we put $X=a\pi$ in (6), then we have the assertion.

§ 2. Congruence for Jacobi sums

As an application of Theorem 1, we shall obtain a new congruence for Jacobi sums (see Theorem 2 below), which generalizes Iwasawa's congruence ([8], Theorem 1 and its remark) and Ihara's congruence ([5], Corollary to Theorem 7).

Conversely, we shall give another proof of Theorem 1 by using Uehara's method of computation on Jacobi sums (see the proof of Lemma 1 in [11]).

Definition. For any integer $r\geqq 1$ and any $a=(a_1, \cdots, a_r)\in \boldsymbol{Z}/m \times\cdots\times \boldsymbol{Z}/m$ (direct product of r copies of $\boldsymbol{Z}/m$), put

$$\begin{aligned} J_a(\mathfrak{p}) &= J(\chi_{\mathfrak{p}}^{a_1}, \cdots, \chi_{\mathfrak{p}}^{a_r}) \\ &= (-1)^{r+1}\sum_{\substack{x_1+\cdots+x_r=-1 \\ x_1,\cdots,x_r\in F_q}}\chi_{\mathfrak{p}}^{a_1}(x_1)\chi_{\mathfrak{p}}^{a_2}(x_2)\cdots\chi_{\mathfrak{p}}^{a_r}(x_r). \end{aligned}$$

For any ideal $\mathfrak{a}$ of $\boldsymbol{Q}(\zeta_m)$ which is prime to m, put

$$J_a(\mathfrak{a})=\prod_{\mathfrak{q}} J_a(\mathfrak{q})^{e_{\mathfrak{q}}},$$

where $\mathfrak{a}=\prod_{\mathfrak{q}}\mathfrak{q}^{e_{\mathfrak{q}}}$ is the prime ideal decomposition of $\mathfrak{a}$. The sum $J_a(\mathfrak{a})$ is called a *Jacobi sum.*

As is well-known, the Jacobi sum is expressed in terms of Gauss sums, as is stated in the following

Lemma 4. *If* $a=(a_1, \cdots, a_r) \not\equiv (0, 0, \cdots, 0) \pmod{m}$, *then*

$$J_a(\mathfrak{p}) = N\mathfrak{p}^{-1} g(a_1) g(a_2) \cdots g(a_r) g\left(-\sum_{i=1}^{r} a_i\right).$$

For the proof, see Weil [14] and Deligne [3].

By using Theorem 1 and Lemma 4, we have directly the following

Theorem 2. *Let the notation and assumptions be as in Theorem* 1 *and let* $a=(a_1, \cdots, a_r) \in \boldsymbol{Z}/l^n \times \cdots \times \boldsymbol{Z}/l^n$ *(the direct product of r copies of* $\boldsymbol{Z}/l^n$*) be such that* $a \not\equiv (0, \cdots, 0) \pmod{l^n}$. *Furthermore, let* $\mathfrak{a}$ *be any ideal of* $\boldsymbol{Q}(\zeta_{l^n})$ *which is prime to l. Then*

$$J_a(\mathfrak{a}) \equiv N\mathfrak{a}^{-1} \cdot \operatorname{Exp}\left\{ \sum_{i=1}^{(l-3)/2} \left(\sum_{j=0}^{r} a_j^{2i+1} \right) \beta_{2i}(\mathfrak{a}) \frac{\pi^{2i+1}}{(2i+1)!} + \frac{N\mathfrak{a}-1}{2l} \left(\sum_{j=0}^{r} a_j^{l-1} \right) \pi^{l-1} \right\} \pmod{\pi^l},$$

where $a_0 = -\sum_{j=1}^{r} a_j$ *and* $\beta_{2i}(\mathfrak{a}) = -[\varepsilon_{2i}, \mathfrak{a}]_l$. *Here we omit the last term if* $l=2$.

Proof. Since $N\mathfrak{a}$ (resp. $[\varepsilon_{2i}, \mathfrak{a}]_l$) is multiplicative (resp. additive) with respect to $\mathfrak{a}$ and since

$$\frac{N\mathfrak{a}-1}{2l} \equiv \frac{1}{2} \frac{1}{l} \log N\mathfrak{a} \pmod{l},$$

we may assume $\mathfrak{a}=\mathfrak{p}$, where log is the l-adic log. Then by Theorem 1 and Lemma 4 we have directly the assertion.

Another proof of Theorem 1. Assume $l \geqq 3$. Put $G = \operatorname{Gal}(\boldsymbol{Q}(\zeta_{l^n})/\boldsymbol{Q})$. Let H be the unique subgroup of G of order $(l-1)$. For each $\tau \in H$, by the definition of $J(\chi_{\mathfrak{p}}, \chi_{\mathfrak{p}}^{\tau})$ and $\lambda(x)$ we have

$$J(\chi_{\mathfrak{p}}, \chi_{\mathfrak{p}}^{\tau}) \equiv -\sum_{\substack{x \in \boldsymbol{F}_q \\ x \neq 0,1}} \chi_{\mathfrak{p}}(x) \zeta_{l^n}^{\omega(\tau)\lambda(1-x)} \pmod{\pi^l},$$

since $\zeta_{l^n}^{l} \equiv 1 \pmod{\pi^l}$. Hence

$$J(\chi_{\mathfrak{p}}, \chi_{\mathfrak{p}}^{\tau}) \equiv -\sum_{\substack{x \in \boldsymbol{F}_q \\ x \neq 0,1}} \chi_{\mathfrak{p}}(x) \operatorname{Exp}(\lambda(1-x)\omega(\tau)\pi) \pmod{\pi^l}$$

$$\equiv 1 + \sum_{j=1}^{l-1} c_j (\omega(\tau)\pi)^j \pmod{\pi^l},$$

where

$$c_1=-\sum_{\substack{x\in F_q\\ x\neq 0,1}}\chi_{\mathfrak{p}}(x)\lambda(1-x) \tag{1}$$

and c_i $(2\leqq i\leqq l-1)$ is an element of $\boldsymbol{Z}_l[\zeta_{l^n}]$ independent of τ. Hence

$$\operatorname{Log} J(\chi_{\mathfrak{p}},\chi_{\mathfrak{p}}^{\tau})\equiv\sum_{j=1}^{l-1}d_j(\omega(\tau)\pi)^j \pmod{\pi^l} \tag{2}$$

with $d_1=c_1$ and some $d_j\in\boldsymbol{Z}_l[\zeta_{l^n}]$ $(2\leqq j\leqq l-1)$ independent of τ. For each $1\leqq i\leqq l-1$, put $\delta_1=\omega^i$ and

$$e_{\delta_1}=\frac{1}{l-1}\sum_{\sigma\in H}\delta_1^{-1}(\sigma)\sigma\in\boldsymbol{Z}_l[H].$$

By making e_{δ_1} operate on both members of (2), we have

$$e_{\delta_1}\operatorname{Log} J(\chi_{\mathfrak{p}},\chi_{\mathfrak{p}}^{\tau})\equiv\sum_{j=1}^{l-1}\omega(\tau)^j e_{\delta_1}(d_j\pi^j) \pmod{\pi^l}. \tag{3}$$

Hence

$$\sum_{\tau\in H}\omega^{-1}(\tau)e_{\delta_1}\operatorname{Log} J(\chi_{\mathfrak{p}},\chi_{\mathfrak{p}}^{\tau})\equiv(l-1)e_{\delta_1}(d_1\pi) \pmod{\pi^l}, \tag{4}$$

since

$$\sum_{\tau\in H}\omega^{j-1}(\tau)=\begin{cases}l-1 & \text{if } j=1,\\ 0 & \text{otherwise.}\end{cases} \tag{5}$$

Since $\sigma\pi\equiv\omega(\sigma)\pi \pmod{\pi^l}$ for $\sigma\in H$, we have

$$e_{\delta_1}\pi^j\equiv\frac{1}{l-1}\left(\sum_{\sigma\in H}\omega(\sigma)^{j-i}\right)\pi^j \pmod{\pi^l},$$

so

$$e_{\delta_1}\pi^j\equiv\begin{cases}\pi^j \pmod{\pi^l} & \text{if } j=i,\\ 0 \pmod{\pi^l} & \text{otherwise,}\end{cases} \tag{6}$$

for $1\leqq j\leqq l-1$. Since

$$d_1\pi\equiv-\sum_{j=0}^{l-1}\beta_j\frac{\pi^{j+1}}{j!} \pmod{\pi^l},$$

by (6) we have

$$e_{\delta_1}(d_1\pi)\equiv-\beta_{i-1}\frac{\pi^i}{(i-1)!} \pmod{\pi^l}, \tag{7}$$

where β_j is as in Lemma 2. By (4) and (7), we have

$$\sum_{\tau\in H}\omega^{-1}(\tau)e_{\delta_1}\operatorname{Log}J(\chi_\mathfrak{p},\chi_\mathfrak{p}^\tau)\equiv\beta_{i-1}\frac{\pi^i}{(i-1)!}\pmod{\pi^l}. \tag{8}$$

On the other hand, by Lemma 4 we have

$$J(\chi_\mathfrak{p},\chi_\mathfrak{p}^\tau)=N\mathfrak{p}^{-1}g(\chi_\mathfrak{p})g(\chi_\mathfrak{p}^\tau)g(\chi_\mathfrak{p}^{-1-\tau}). \tag{9}$$

Since we can write

$$g(\chi_\mathfrak{p})\equiv\operatorname{Exp}\left(\sum_{j=1}^{l-1}\lambda_j\frac{\pi^j}{j!}\right)\pmod{\pi^l}$$

with some $\lambda_j\in\boldsymbol{Z}_l[\zeta_p]$, by making $\tau\in H$ operate on both members we have

$$g(\chi_\mathfrak{p}^\tau)\equiv\operatorname{Exp}\left(\sum_{j=1}^{l-1}\lambda_j\frac{(\omega(\tau)\pi)^j}{j!}\right)\pmod{\pi^l}$$

for any $\tau\in H$. Here we identify $\mathrm{G}(\boldsymbol{Q}(\zeta_{l^np})/\boldsymbol{Q}(\zeta_p))$ and G by restriction. Since $g(\chi_\mathfrak{p}^c)\pmod{\pi^l}$ depends only on $c\pmod{l}$ as is seen in the beginning of the proof of Theorem 1, we have

$$g(\chi_\mathfrak{p}^c)\equiv\operatorname{Exp}\left(\sum_{j=1}^{l-1}\lambda_j\frac{(c\pi)^j}{j!}\right)\pmod{\pi^l} \tag{10}$$

for any $c\in\boldsymbol{Z}_l$. By (9) and (10) we have

$$J(\chi_\mathfrak{p},\chi_\mathfrak{p}^\tau)\equiv N\mathfrak{p}^{-1}\operatorname{Exp}\left(\sum_{j=1}^{l-1}\lambda_j\gamma_j(\tau)\frac{\pi^j}{j!}\right)\pmod{\pi^l},$$

where $\gamma_j(\tau)=1+\omega(\tau)^j+(-1)^j(1+\omega(\tau))^j$. Hence

$$\operatorname{Log}J(\chi_\mathfrak{p},\chi_\mathfrak{p}^\tau)\equiv-\operatorname{Log}N\mathfrak{p}+\sum_{j=1}^{l-1}\lambda_j\gamma_j(\tau)\frac{\pi^j}{j!}\pmod{\pi^l}. \tag{11}$$

By making e_{δ_1} operate on both members of (11) and using (6), we have

$$e_{\delta_1}\operatorname{Log}J(\chi_\mathfrak{p},\chi_\mathfrak{p}^\tau)\equiv\begin{cases}\lambda_i\gamma_i(\tau)\dfrac{\pi^i}{i!} & \pmod{\pi^l}\text{ if }1\leqq i\leqq l-2,\\ \lambda_i\gamma_i(\tau)\dfrac{\pi^i}{i!}-\operatorname{Log}N\mathfrak{p} & \pmod{\pi^l}\text{ if }i=l-1.\end{cases} \tag{12}$$

Since

$$\gamma_i(\tau)=1+(-1)^i\sum_{k=0}^{i}\binom{i}{k}\omega(\tau)^k+\omega(\tau)^i,$$

by (5) we have

$$(13)\qquad \sum_{\tau\in H}\omega^{-1}(\tau)e_{\delta_1}\operatorname{Log}J(\chi_{\mathfrak{p}},\chi_{\mathfrak{p}}^{\tau})\equiv(-1)^{i-1}\lambda_i\frac{\pi^i}{(i-1)!}\qquad(\mathrm{mod}\ \pi^l)$$

for $2\leqq i\leqq l-1$. By (8) and (13) we have

$$\lambda_i\equiv(-1)^{i-1}\beta_{i-1}\qquad(\mathrm{mod}\ l)$$

for $2\leqq i\leqq l-1$. Hence by Lemmas 2 and 3 we have

$$\lambda_i\equiv\begin{cases}-[\varepsilon_{i-1},\mathfrak{p}]_l\ (\mathrm{mod}\ l) & \text{if } i\ (3\leqq i\leqq l-2) \text{ is odd,}\\ 0\ \ (\mathrm{mod}\ l) & \text{if } i\ (2\leqq i\leqq l-3) \text{ is even,}\\ (q-1)/2l\ \ (\mathrm{mod}\ l) & \text{if } i=l-1.\end{cases}$$

We have $\lambda_1=\alpha_1$ as in the beginning of the proof of Theorem 1. Hence by (10) we have the assertion.

Note. Ihara [5] created the theory of "universal" power series for Jacobi sums, and he gave his intensive lecture about his interesting theory at Tokyo Metropolitan University in Dec. 1984. Meanwhile, we understood that the problem of the determination of the coefficients of Ihara's power series $F_\rho(u, v)$ is closely related to our problem of the l-adic expansion of Gauss sums. We denote by Ω_l the maximum abelian l-extension of the cyclotomic field $\boldsymbol{Q}(\mu_{l^\infty})$ (μ_{l^∞} is the group of all l-th power roots of unity in $\boldsymbol{C}$) unramified outside l, and by Ω_l^{ur} the maximum unramified sub-extension of $\Omega_l/\boldsymbol{Q}(\mu_{l^\infty})$, and put

$$\mathfrak{g}_2=\mathrm{Gal}\,(\Omega_l/\Omega_l^{\mathrm{ur}})\subset\mathfrak{g}_1=\mathrm{Gal}\,(\Omega_l/\boldsymbol{Q}(\mu_{l^\infty}))\subset\mathfrak{g}_0=\mathrm{Gal}\,(\Omega_l/\boldsymbol{Q}).$$

Ihara ([5], Theorem 10 and its Corollary) determined the coefficients of $F_\rho(u, v)$ for $\rho\in\mathfrak{g}_2$, and he conjectured that the same formula holds for $\rho\in\mathfrak{g}_1$. We also understood that if Ihara's conjecture can be generalized for $\rho\in\mathfrak{g}_0$ and if it can be proved, then we might be able to give another proof of our Theorems 1 and 2 by using this and Theorem 7 of Ihara [5]. But, at that time, Ihara's conjecture was proved only for $\rho\in\mathfrak{g}_2$, so there was some gap between his formula and our Theorem 2. This is a reason why a weaker result for the congruence for Jacobi sums (Ihara [5], Corollary to Theorem 7) was obtained. Meanwhile, during the Kyoto conference in Oct. 1985, by using Iwasawa's theory, Coleman [2] obtained a proof of Ihara's conjecture for $\rho\in\mathfrak{g}_1$, and later a more general formula for $\rho\in\mathfrak{g}_0$.

Thus it became possible for Coleman and Anderson [1] to give another proof of our Theorems 1 and 2. So, as is stated in the introduction, we have four different proofs of our Theorems 1 and 2, and we note that our original proof of Theorems 1 and 2 is the most elementary one. We also note that after the Kyoto conference Ihara-Kaneko-Yukinari [6] obtained another proof of Ihara's conjecture for $\rho \in \mathfrak{g}_1$ in a different method from Coleman [2].

§ 3. Algebraic proof of the nonvanishing of certain character sums in certain cases

Let $m>1$ be any integer. We identitfy $G=\mathrm{G}(\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q})$ and $(\boldsymbol{Z}/m)^\times$ by $\sigma_b \leftrightarrow b \bmod m$, where $\sigma_b \in G$ is such that $\zeta_m^{\sigma_b}=\delta_m^b$. Let $\hat{G}$ be the character group of G. The function ϕ on $\boldsymbol{Z}$ with values in $\boldsymbol{C}$ is called the *Dirichlet character* defined modulo m if it satisfies the following (i), (ii) and (iii):

(i) $\phi(bc)=\phi(b)\phi(c)$ for any $b, c \in \boldsymbol{Z}$.
(ii) $\phi(b)=\phi(c)$ if $b \equiv c \pmod m$.
(iii) $\phi(b)=0$ if and only if $(b, m) \neq 1$.

We identify $\phi \in \hat{G}$ and the Dirichlet character defined modulo m by

$$\phi(b)=\begin{cases}\phi(\sigma_b) & \text{if } (b, m)=1,\\ 0 & \text{otherwise.}\end{cases}$$

ϕ ($\in \hat{G}$) is called *even* (resp. *odd*) if $\phi(\sigma_{-1})=\phi(-1)=1$ (resp. -1). ϕ is even (resp. odd) if and only if K_ϕ is real (resp. imaginary), where K_ϕ is the fixed field of $\mathrm{Ker}\,\phi$ in $\boldsymbol{Q}(\zeta_m)$ by Galois theory.

Let $\delta \in \hat{G}$ be any odd character and let g be the order of δ. Then $G/\mathrm{Ker}\,\delta \cong \mathrm{Im}\,\delta=\langle\zeta_g\rangle$ (cyclic group generated by ζ_g). Let s_δ be a representative element of a generator of $G/\mathrm{Ker}\,\delta$ and we fix s_δ.

Definition. Put

$$\alpha_\delta=\Big(\sum_{\sigma \in \mathrm{Ker}\,\delta}\sigma\Big)\prod_{p'}(1-s_\delta^{g/p'}) \in Z[G],$$

where the product is taken over all prime numbers p' such that $p'|g$.

The following lemma 5 due to Ullom [12] is our starting point.

Lemma 5. *Put*

$$\xi=\sum_{\substack{a=1\\(a,m)=1}}^{m} a\sigma_a^{-1} \in \boldsymbol{Z}[G].$$

Let $\delta \in \hat{G}$ be any odd Dirichlet character defined modulo m and let $\alpha_\delta \in \boldsymbol{Z}[G]$

be as above. Put

$$M(\delta)=\sum_{a=1}^{m} a\delta(a).$$

Then the following (i) *and* (ii) *are equivalent.*

(i) $M(\delta)=0$.

(ii) $\xi\alpha_\delta=0$ *in* $\boldsymbol{Z}[G]$.

Using Lemma 5 and Stickelberger's theorem we can prove the following key lemma.

Lemma 6. *Let* $g(\chi_\mathfrak{p})$ *be the Gauss sum defined in the introduction. Then for any odd character* $\delta\in\hat{G}$, *the following* (i) *and* (ii) *are equivalent.*

(i) $M(\delta)=0$.

(ii) $g(\chi_\mathfrak{p}^a)^{\alpha_\delta}=\pm\zeta_m^i$ *with some* $i\in\boldsymbol{Z}$, *for any* (*resp. some*) *prime ideal* $\mathfrak{p}$ *of* $\boldsymbol{Q}(\zeta_m)$ (*resp. which is completely decomposed with respect to* $\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}$) *such that* $(\mathfrak{p}, m)=1$ *and for any* (*some*) $a\in\boldsymbol{Z}$ *such that* $(a, m)=1$. *Here we identify* $G(\boldsymbol{Q}(\zeta_{mp})/\boldsymbol{Q}(\zeta_p))$ *and* G *by restriction, where* p *is a prime number such that* $p\in\mathfrak{p}$.

Proof. Since $g(\chi_\mathfrak{p})^{\sigma_a}=g(\chi_\mathfrak{p}^a)$, we may assume $a=-1$. By Stickelberger's theorem, we have

$$(g(\chi_\mathfrak{p}^{-1})^m)=\mathfrak{p}^\xi, \tag{1}$$

where $(g(\chi_\mathfrak{p}^{-1})^m)$ is a principal ideal generated by $g(\chi_\mathfrak{p}^{-1})^m$ and ξ is as in Lemma 5. Note that $g(\chi_\mathfrak{p}^{-1})^m\in\boldsymbol{Q}(\zeta_m)$ as is well-known. Put $A=g(\chi_\mathfrak{p}^{-1})^m$. By Lemma 5, $M(\delta)=0$ if and only if $\xi\alpha_\delta=0$, i.e., $\mathfrak{p}^{\xi\alpha_\delta}=1$ for some $\mathfrak{p}$ which is completely decomposed in $\boldsymbol{Q}(\zeta_m)/\boldsymbol{Q}$. Hence, by making α_δ operate on the both members of (1), we see that (i) is equivalent to that $(A)^{\alpha_\delta}=1$, i.e., A^{α_δ} is a unit of $\boldsymbol{Q}(\zeta_m)$. Hence (ii) implies (i). Now assume (i), and put $\varepsilon=A^{\alpha_\delta}$. Then ε is a unit of $\boldsymbol{Q}(\zeta_m)$, and we have $|\varepsilon|^2=1$, since

$$g(\chi_\mathfrak{p}^{-1})\overline{g(\chi_\mathfrak{p}^{-1})}=q.$$

Hence ε is a root of unity in $\boldsymbol{Q}(\zeta_m)$, i.e., $g(\chi_\mathfrak{p}^{-1})^{\alpha_\delta}$ is a root of unity in $\boldsymbol{Q}(\zeta_{mp})$. Hence we can write

$$g(\chi_\mathfrak{p}^{-1})^{\alpha_\delta}=\pm\zeta_{mp}^i \tag{2}$$

with some $i\in\boldsymbol{Z}$, where $\zeta_{mp}=\zeta_m\zeta_p$. Since $g(\chi_\mathfrak{p}^{-1})^m\in\boldsymbol{Q}(\zeta_m)$, by (2) we have $(\pm\zeta_{mp}^i)^m\in\boldsymbol{Q}(\zeta_m)$, so $\zeta_p^{im}\in\boldsymbol{Q}(\zeta_m)$. Since $(m, p)=1$, we have $i\equiv 0 \pmod p$. Hence we have (i).

Lemma 7. *Let* l *be any prime number and let* α_1 *be as in Theorem* 1.

Let $\tau \in \mathrm{Gal}(\boldsymbol{F}_l(\bar{\zeta}_p)/\boldsymbol{F}_l)$ *be the l-th power isomorphism of* $\boldsymbol{F}_l(\bar{\zeta}_p)$, *where* $\bar{\zeta}_p = \zeta_p \bmod l\boldsymbol{Z}_l[\zeta_p]$. *Then we have*

$$\alpha_1^\tau = \alpha_1 + \lambda(l).$$

In particular, we have $\alpha_1 \notin \boldsymbol{F}_l$ *if* $\lambda(l) \neq 0$.

Proof. Since

$$\begin{aligned}\alpha_1^\tau &= -\sum_{x \in \boldsymbol{F}_q^\times} \lambda(x)\psi(lx) \\ &= -\sum_{y \in \boldsymbol{F}_q^\times} \lambda(l^{-1}y)\psi(y),\end{aligned}$$

we have

$$\alpha_1^\tau = \alpha_1 + \lambda(l).$$

The last statement follows from this.

Lemma 8. *Let l be any prime number and put* $m = l^n$ *with* $n \geqq 1$. *Let* $\lambda_\mathfrak{p}$ *be as in Section* 1. *Then there exist infinitely many prime ideals* $\mathfrak{p}$ *of degree* 1 *in* $\boldsymbol{Q}(\zeta_m)$ *not lying above l such that* $\lambda_\mathfrak{p}(l) \neq 0$.

Proof. We have $\lambda_\mathfrak{p}(l) \neq 0$ if and only if $l \bmod \mathfrak{p} \notin (\boldsymbol{F}_q^\times)^l$, so $\mathfrak{p}$ is unramified and not decomposed in $\boldsymbol{Q}(\zeta_m)(\sqrt[l]{l})/\boldsymbol{Q}(\zeta_m)$. By Čebotarev's density theorem, there exist infinitely many such $\mathfrak{p}$ (Wojcik [17] gives a purely algebraic proof of Čebotarev's density theorem in the special case which covers our case).

Lemma 9. *Let l be any odd prime number and let n be any natural number. Let* π *be a prime element of* $\boldsymbol{Q}_l(\zeta_{l^n})$ *as in Section* 1 *and let* δ *be a primitive Dirichlet character of conductor* l^n. *Put*

$$\alpha'_\delta = \Big(\sum_{\sigma \in \mathrm{Ker}\,\delta} \sigma\Big) \prod_{\substack{p' \mid g \\ p' \neq l}} (1 - s_\delta^{g/p'}) \in \boldsymbol{Z}[G],$$

where the notation is as in the beginning of Section 3 *and the product is taken over all prime numbers* p' *such that* $p' \mid g$ *and* $p' \neq l$. *Let H be the unique subgroup of G of order* $(l-1)$ *and let* ω_0 *be the restriction of* ω *to H. Here we consider the Teichmüller character* ω *as a character of G in the natural way. Then we have*

$$\alpha'_\delta \pi^j \equiv \lambda_j(\delta)\pi^j \pmod{\pi^l} \qquad \text{for } 1 \leqq j < l,$$

where

$$\lambda_j(\delta)=\Big(\sum_{\sigma\in\mathrm{Ker}\,\delta}\omega^j(\sigma)\Big)\prod_{\substack{p'\mid g\\ p'\neq l}}(1-\omega^j(s_\delta^{g/p'}))\in \boldsymbol{Z}_l.$$

Here we have $\lambda_j(\delta)\not\equiv 0 \pmod{l\boldsymbol{Z}_l}$ *if and only if* $\mathrm{Ker}\,\delta=\mathrm{Ker}\,\omega_0^j$.

Proof. Since

$$\pi^{\sigma a}\equiv\omega(a)\pi \pmod{\pi^l} \tag{1}$$

for $a\in\boldsymbol{Z}$, $a\not\equiv 0 \pmod l$, we have

$$\alpha'^{\,j}_\delta\pi^j\equiv\lambda_j(\delta)\pi^j \pmod{\pi^l}.$$

Since δ is primitive, we have $\mathrm{Ker}\,\delta\subset H$. If $\omega_0^j|_{\mathrm{Ker}\,\delta}\neq 1$, then

$$\sum_{\sigma\in\mathrm{Ker}\,\delta}\omega^j(\sigma)=0,$$

so $\lambda_j(\delta)=0$. If $\mathrm{Ker}\,\omega_0^j\supsetneq\mathrm{Ker}\,\delta$, then there exists a prime number p' dividing $(\mathrm{Ker}\,\omega_0^j\colon\mathrm{Ker}\,\delta)$, so $(H\colon\mathrm{Ker}\,\delta)$. Hence $p'\mid g$, $p'\neq l$ and $s_\delta^{g/p'}\in\mathrm{Ker}\,\omega_0^j$. Thus $1-\omega^j(s_\delta^{g/p'})=0$, so $\lambda_j(\delta)=0$. If $\mathrm{Ker}\,\omega_0^j=\mathrm{Ker}\,\delta$, then ω_0^j induces the natural isomorphism $H/\mathrm{Ker}\,\delta\cong\langle\zeta_{g'}\rangle$, where $g'=g/l^{n-1}\not\equiv 0 \pmod l$. Since the order of $s_\delta^{g/p'}$ mod $\mathrm{Ker}\,\delta$ is p' and since $p'\neq l$, we see that $s_\delta^{g/p'}\in H$ and that $\omega^j(s_\delta^{g/p'})$ is a primitive p'-th root of unity. Hence

$$1-\omega^j(s_\delta^{g/p'})\not\equiv 0 \pmod{l\boldsymbol{Z}_l}.$$

Since $\sum_{\sigma\in\mathrm{Ker}\,\delta}\omega^j(\sigma)=|\mathrm{Ker}\,\delta|\not\equiv 0 \pmod{l\boldsymbol{Z}_l}$, we have $\lambda_j(\delta)\not\equiv 0 \pmod{l\boldsymbol{Z}_l}$.

For the proof of Lemma 11, we need the following well known lemma (e.g. Weil [16], Chap. XIII, § 8, Lemma 9).

Lemma 10. *Let l be any prime number and let K be a field of characteristic different from l. For $n\geqq 1$, let ζ_{l^n} be a primitive l^n-th root of unity and put $K_n=K(\zeta_{l^n})$. If $l=2$, assume $\zeta_4\in K$. Then $K^\times\cap(K_n^\times)^{l^n}=(K^\times)^{l^n}$ for all $n\geqq 1$.*

Lemma 11. *Let l be any prime number and let δ, α'_δ be as in Lemma 9. Assume that $n\geqq 2$ or $n\geqq 3$ according as $l\geqq 3$ or $l=2$. Furthermore, assume $M(\delta)=0$, where $M(\delta)$ is as in Lemma 5. Then we can write*

$$g(\chi_p)^{\alpha'_\delta}=z\zeta_{l^n}^i$$

with some $z\in\boldsymbol{Q}(\zeta_{l^{n-1}p})$ and some $i\in Z$. In particular,

$$g(\chi_p)^{\alpha'_\delta}\equiv\zeta_{l^n}^i \pmod{\pi^l}$$

with some $i\in\boldsymbol{Z}$.

Proof. By assumption and Lemma 6, we have

$$g(\chi_\mathfrak{p})^{\alpha_\delta} = \pm\zeta_{l^n}^i$$

with some $i \in \boldsymbol{Z}$. Since $g(\chi_\mathfrak{p}) \equiv 1 \pmod{\pi}$ and since $\zeta_{2^n}^{2^{n-1}} = -1$, we can write

$$g(\chi_\mathfrak{p})^{\alpha_\delta} = \zeta_{l^n}^i$$

with some $i \in \boldsymbol{Z}$, so

$$(g(\chi_\mathfrak{p})^{l^n})^{\alpha_\delta} = 1. \tag{1}$$

Since $\alpha_\delta = \alpha'_\delta(1 - s_\delta^{g/l})$, by (1) we have

$$(g(\chi_\mathfrak{p})^{l^n})^{\alpha'_\delta} \in \boldsymbol{Q}(\zeta_{l^{n-1}p}).$$

By using Lemma 10 for $K = \boldsymbol{Q}(\zeta_{l^{n-1}p})$, we can write

$$(g(\chi_\mathfrak{p})^{\alpha'_\delta})^{l^n} = z^{l^n}$$

with some $z \in \boldsymbol{Q}(\zeta_{l^{n-1}p})$, so

$$g(\chi_\mathfrak{p})^{\alpha'_\delta} = z\zeta_{l^n}^i \tag{2}$$

with some $i \in \boldsymbol{Z}$. Since $\boldsymbol{Q}_l(\zeta_{l^n p})/\boldsymbol{Q}_l(\zeta_{l^{n-1}p})$ is a fully ramified cyclic extension of degree l, (2) implies the last assertion.

§ 3.1. The case where $m = l^n$ and $\operatorname{Ker}\delta = \{1\}$

In this section, we assume that $m = l^n$ and $\operatorname{Ker}\delta = \{1\}$ where l is any prime number and $n \geqq 1$.

An algebraic proof of $M(\delta) \neq 0$ in the case where $m = l^n$ and $\operatorname{Ker}\delta = \{1\}$.

Since $\operatorname{Ker}\delta = \{1\}$, we have $G \cong (\boldsymbol{Z}/m)^\times \cong \operatorname{Im}\delta$, so $(\boldsymbol{Z}/m)^\times$ is a cyclic group. Hence, if $l = 2$, then we have $n = 1$, so $M(\delta) = 1$. Hence we may assume $l \geqq 3$. By Lemma 8, there exists a prime ideal $\mathfrak{p}$ of degree 1 in $\boldsymbol{Q}(\zeta_m)$ such that $\lambda_\mathfrak{p}(l) \neq 0$. Then by Lemma 7, we have $\alpha_1 \notin \boldsymbol{F}_l$. By Lemma 6 for $n = 1$ and Lemma 11 for $n > 1$, we have

$$g(\chi_\mathfrak{p})^{\alpha'_\delta} \equiv \zeta_{l^n}^i \pmod{\pi^l} \tag{1}$$

with some $i \in \boldsymbol{Z}$. On the other hand, by Theorem 1 and Lemma 9, we have

$$g(\chi_\mathfrak{p})^{\alpha'_\delta} \equiv 1 + \alpha_1\lambda_1(\delta)\pi \pmod{\pi^2}. \tag{2}$$

Since $\operatorname{Ker}\delta = \operatorname{Ker}\omega_0 = \{1\}$, by Lemma 9 we have

$$\lambda_1(\delta)\not\equiv 0 \pmod{l\boldsymbol{Z}_l}. \tag{3}$$

By (1) and (2), we have

$$\alpha_1\lambda_1(\delta)\equiv i \pmod{l\boldsymbol{Z}_l[\zeta_p]},$$

so by (3), we have $\alpha_1 \in \boldsymbol{F}_l$. This is a contradiction.

§ 3.2. The case where $m=l^n$ and the order of δ is 2^t with $t\geqq 1$

In this section, let l be any prime number and put $m=l^n$ with $n\geqq 1$. Let δ be a primitive odd Dirichlet character of conductor l^n and of order 2^t with $t\geqq 1$.

An algebraic proof of $M(\delta)\not\equiv 0$ in the above case.

First assume $l\geqq 3$. Then $n=1$. Let K_δ be the fixed field by $\operatorname{Ker}\delta$ in $\boldsymbol{Q}(\zeta_l)$. Since $\delta(-1)=-1$ and the order of δ is 2^t, we see that $s_\delta^{2^{t-1}}$ is equal to σ_{-1} on K_δ, so we have

$$g(\chi_\mathfrak{p})^{l\alpha_\delta}=N_{\boldsymbol{Q}(\zeta_l)/K_\delta}(g(\chi_\mathfrak{p})^l)^{1-\sigma_{-1}}. \tag{1}$$

Suppose $M(\delta)=0$. Then by Lemma 6,

$$g(\chi_\mathfrak{p})^{\alpha_\delta}=\pm\zeta_l^i$$

with some $i\in\boldsymbol{Z}$. Since $g(\chi_\mathfrak{p})\equiv 1 \pmod{\pi}$, we have

$$g(\chi_\mathfrak{p})^{\alpha_\delta}=\zeta_l^i,$$

so

$$(g(\chi_\mathfrak{p})^l)^{\alpha_\delta}=1. \tag{2}$$

Hence by (1) we see that $N_{\boldsymbol{Q}(\zeta_l)/K_\delta}(g(\chi_\mathfrak{p})^l)$ is real. Since $g(\chi_\mathfrak{p})\overline{g(\chi_\mathfrak{p})}=q$, this implies

$$N_{\boldsymbol{Q}(\zeta_l)/K_\delta}(g(\chi_\mathfrak{p})^l)^2=q^{sl},$$

where $s=[\boldsymbol{Q}(\zeta_l):K_\delta]\not\equiv 0 \pmod 2$. Hence we see that $\sqrt{q}\in\boldsymbol{Q}(\zeta_l)$. By Čebotarev's density theorem, there exist infinitely many prime numbers p which are completely decomposed in $\boldsymbol{Q}(\zeta_l)/\boldsymbol{Q}$, i.e., $p\equiv 1 \pmod l$ (In this case, an elementary proof is known. See Washington [13], Corollary 2.11). Then $q=p$. Since p is fully ramified in $\boldsymbol{Q}(\sqrt{p})/\boldsymbol{Q}$ and since p is unramified in $\boldsymbol{Q}(\zeta_l)/\boldsymbol{Q}$, this is a contradiction. Hence $M(\delta)\not\equiv 0$. Now assume $l=2$. If $n=2$, then it is clear that $M(\delta)\not\equiv 0$. Hence we may assume $n\geqq 3$. Since the conductor of δ is 2^n, we have

$$\operatorname{Ker}\delta=\{1,\sigma\sigma_{-1}\},$$

where $\sigma=\sigma_5^{2^{n-3}}$ is a generator of $G(\boldsymbol{Q}(\zeta_{2^n})/\boldsymbol{Q}(\zeta_{2^{n-1}}))$. Assume $M(\delta)=0$. Then by Lemma 11 we have

$$g(\chi_\mathfrak{p})^{\alpha'_\delta}=z\zeta_{2^n}^i \tag{3}$$

with some $z\in\boldsymbol{Q}(\zeta_{2^{n-1}p})$ and some $i\in\boldsymbol{Z}$, where $\alpha'_\delta=1+\sigma\sigma_{-1}$. Since $\pi^{\sigma_a}\equiv a\pi \pmod{\pi^2}$ for $a\in\boldsymbol{Z}$, $a\not\equiv 0 \pmod 2$, by Theorem 1 we have

$$g(\chi_\mathfrak{p})^{\alpha'_\delta}\equiv 1 \pmod{\pi^2}. \tag{4}$$

Since $\boldsymbol{Q}_2(\zeta_{2^np})/\boldsymbol{Q}_2(\zeta_{2^{n-1}p})$ is a fully ramified quadratic extension, by (3) and (4) we have

$$g(\chi_\mathfrak{p})^{\alpha'_\delta}\in\boldsymbol{Q}(\zeta_{2^{n-1}p}). \tag{5}$$

This implies that $g(\chi_\mathfrak{p})^{\alpha'_\delta}$ is invariant by σ and $\sigma\sigma_{-1}$, hence by σ_{-1}, so

$$g(\chi_\mathfrak{p})^{(1-\sigma_{-1})(\sigma-1)}=1. \tag{6}$$

Since $g(\chi_\mathfrak{p})^{1+\sigma_{-1}}=\pm q$, this implies

$$(g(\chi_\mathfrak{p})^{\sigma-1})^2=1,$$

so

$$g(\chi_\mathfrak{p})^{\sigma-1}=(-1)^j$$

with some $j\in\boldsymbol{Z}$. Since $\zeta_{2^n}^\sigma=-\zeta_{2^n}$, we have

$$(g(\chi_\mathfrak{p})\zeta_{2^n}^j)^{1-\sigma}=1,$$

so

$$g(\chi_\mathfrak{p})\zeta_{2^n}^j\in\boldsymbol{Q}(\zeta_{2^{n-1}p}). \tag{7}$$

Since

$$g(\chi_\mathfrak{p})\equiv 1+\alpha_1\pi \pmod{\pi^2}$$

by Theorem 1, we have

$$\begin{aligned} g(\chi_\mathfrak{p})\zeta_{2^n}^j &\equiv(1+\alpha_1\pi)(1+\pi)^j \pmod{\pi^2} \\ &\equiv 1+(\alpha_1+j)\pi \pmod{\pi^2}. \end{aligned} \tag{8}$$

Since $\boldsymbol{Q}_2(\zeta_{2^np})/\boldsymbol{Q}_2(\zeta_{2^{n-1}p})$ is a fully ramified quadratic extension, by (7) and (8) we have

$$\alpha_1+j\equiv 0 \pmod{\pi}.$$

so $\alpha_1 \in \boldsymbol{F}_2$. By Lemmas 7 and 8, this is a contradiction. Thus $M(\delta) \neq 0$.

§ 3.3. The case where $m=l^n$ $(n \geqq 1)$ and $\varepsilon_{\omega\delta_1^{-1}} \notin \boldsymbol{Q}(\zeta_l)^l$ with a prime number $l \geqq 5$

Let δ be a primitive odd Dirichlet character of conductor $m=l^n$ $(n \geqq 1)$ with a prime number $l \geqq 5$. We can decompose δ uniquely into the product:

$$\delta = \delta_1 \delta_2,$$

where δ_1 is a character of the first kind and δ_2 is a character of the second kind (see Iwasawa [7], Section 6, p. 66).

Assume the following condition

(*) $\delta_1 \neq \omega$ and $\varepsilon_{\omega\delta_1^{-1}} \notin \boldsymbol{Q}(\zeta_l)^l$.

Iwasawa [9] gives an algebraic proof of $M(\delta) \neq 0$ under the above condition (*) when $n=1$, by using Artin-Hasse's explicit formula on the norm residue symbol in local class field theory.

In the following, we shall give an *elementary algebraic* proof of $M(\delta) \neq 0$ under the above condition (*) for *any* $n \geqq 1$ by using Theorem 1. Here, "elementary" means that we do not use class field theory.

Algebraic proof of $M(\delta) \neq 0$ *under the above condition* (*) *for any* $n \geqq 1$.

In the case where $\operatorname{Ker}\delta = \{1\}$, we have already given an algebraic proof of $M(\delta) \neq 0$ in Section 3.1. Hence we may assume that $\operatorname{Ker}\delta \neq \{1\}$. Suppose $M(\delta)=0$. Then by Lemmas 6 and 11, we have

$$g(\chi_{\mathfrak{p}})^{\alpha'_\delta} \equiv \pm\zeta_{l^n}^i \pmod{\pi^l} \tag{1}$$

with some $i \in \boldsymbol{Z}$. On the other hand, by Lemma 9 we have

$$g(\chi_{\mathfrak{p}})^{\alpha'_\delta} \equiv 1 \pmod{\pi^2}, \tag{2}$$

since $\operatorname{Ker}\delta \neq \{1\}$. By (1) and (2) we have

$$g(\chi_{\mathfrak{p}})^{\alpha'_\delta} \equiv 1 \pmod{\pi^l}. \tag{3}$$

On the other hand, by Theorem 1 and Lemma 9,

$$g(\chi_{\mathfrak{p}})^{\alpha'_\delta} \equiv \operatorname{Exp}\left(\sum_j \beta_{2j} \frac{\pi^{2j+1}}{(2j+1)!} \lambda_{2j+1}(\delta)\right) \pmod{\pi^l}, \tag{4}$$

where the sum is taken over all j $(1 \leqq j \leqq (l-3)/2)$ such that $\operatorname{Ker}\omega^{2j+1} = \operatorname{Ker}\delta_1$. Since δ_1 is odd and $\delta_1 \neq \omega$, we can write $\delta_1 = \omega^{2i+1}$ with some i $(1 \leqq i \leqq (l-3)/2)$. Then by Lemma 9,

$$\lambda_{2i+1}(\delta) \not\equiv 0 \pmod{l\boldsymbol{Z}_l}. \tag{5}$$

By Čebotarev's density theorem, there exist infinitely many $\mathfrak{p}$ such that

$$\beta_{2i} \not\equiv 0 \pmod{l}. \tag{6}$$

Note that Wojcik [17] gives a purely algebraic proof of Čebotarev's density theorem in the special case which covers our case. By (4), (5) and (6), we have

$$g(\chi_{\mathfrak{p}})^{\alpha'_\delta} \not\equiv 1 \pmod{\pi^l}.$$

This contradicts (3). Hence $M(\delta) \not\equiv 0$.

§ 4. A necessary and sufficient condition for $\varepsilon_\phi \in \boldsymbol{Q}(\zeta_l)^l$ due to Iwasawa

Let $l \geqq 5$ be a prime number and let I be the multiplicative group of all ideals in $\boldsymbol{Q}(\zeta_l)$ which are prime to l. Let P be the subgroup of all principal ideals in I and let I' be the subgroup of I containing P such that I'/P is the Sylow l-subgroup of I/P. Let P' be the subgroup of all principal ideals (α) in P such that $\alpha \equiv 1 \pmod{\pi^{l+1}}$, and put $Y = I'/P'$. Put $G = G(\boldsymbol{Q}(\zeta_l)/\boldsymbol{Q})$. Then Y becomes a G-module which is an abelian l-group. Let Y_δ be the δ-component of Y. i.e., $Y_\delta = e_\delta Y$ for $\delta \in \hat{G}$.

Under the above notation and assumptions, Iwasawa proves the following

Theorem 3 (Iwasawa [9], Lemma 3). *Let ϕ be an even character of G such that $\phi \not\equiv 1$, and put $\delta = \omega\phi^{-1}$. Then $\varepsilon_\phi \in \boldsymbol{Q}(\zeta_l)^l$ if and only if $l^{m(\delta)} Y_\delta = 0$, where $l^{m(\delta)+1}$ is the exact power of l dividing $M(\delta^{-1})$ and $M(\delta^{-1})$ is as in Lemma 5.*

By using Theorem 1 and Stickelberger's theorem we give another proof of the above theorem.

Another proof of Theorem 3. By Stickelberger's theorem we have

$$(g(\chi_{\mathfrak{p}}^{-1})^l) = \mathfrak{p}^\xi \tag{1}$$

for any prime ideal $\mathfrak{p} \in I$, where $\xi = \sum_{a=1}^{l-1} a\sigma_a^{-1} \in \boldsymbol{Z}[G]$. Let $\tilde{e}_\delta \in \boldsymbol{Z}[G]$ be such that $e_\delta \equiv \tilde{e}_\delta \pmod{l^N \boldsymbol{Z}_l[G]}$ for a sufficiently large N. Put $h' = [I : I']$. Then $h' \not\equiv 0 \pmod{l}$. Since $\tilde{e}_\delta \xi \equiv M(\delta^{-1})\tilde{e}_\delta \pmod{l^N}$, we have

$$\tilde{e}_\delta \xi \equiv l^{m(\delta)+1} d\tilde{e}_\delta \pmod{l^N} \tag{2}$$

with some $d \geqq 1$, $(d, l) = 1$. Since $\mathfrak{p}^{h'} \in I'$, we have

$$\mathfrak{p}^{h'lN}=(\alpha^l) \tag{3}$$

with some $\alpha \in \boldsymbol{Q}(\zeta_l)$ such that $\alpha \equiv 1 \pmod{\pi^M}$ for a sufficiently large M, by using the fact that each principal ideal in P is generated by an element α in $\boldsymbol{Q}(\zeta_l)$ such that $\alpha \equiv 1 \pmod{\pi}$ as is stated in Iwasawa [9], p. 118. By making $h'\tilde{e}_\delta$ operate on both members of (1) and using (2) and (3), we have

$$\mathfrak{p}^{h'\tilde{e}_\delta l^{m(\delta)+1}d}=(g(\chi_\mathfrak{p}^{-1})^{h'l\tilde{e}_\delta}\alpha^l)$$

with some $\alpha \in \boldsymbol{Q}(\zeta_l)$ such that $\alpha \equiv 1 \pmod{\pi^M}$ for a sufficiently large M, so

$$\mathfrak{p}^{h'\tilde{e}_\delta l^{m(\delta)}d}=(g(\chi_\mathfrak{p}^{-1})^{\tilde{e}_\delta h'}\alpha). \tag{4}$$

For $b \in \boldsymbol{Z}$, $(b, p)=1$, let $\tau_b \in G(\boldsymbol{Q}(\zeta_{lp}))/\boldsymbol{Q}(\zeta_l))$ be such that $\zeta_p^{\tau_b}=\zeta_p^b$. Since

$$g(\chi_\mathfrak{p}^{-1})^{\tau_b}=\chi_\mathfrak{p}(b)g(\chi_\mathfrak{p}^{-1})$$

and since $\delta \neq \omega$, we have

$$(g(\chi_\mathfrak{p}^{-1})^{\tilde{e}_\delta})^{\tau_b}=g(\chi_\mathfrak{p}^{-1})^{\tilde{e}_\delta}, \text{ i.e.,}$$

$$g(\chi_\mathfrak{p}^{-1})^{\tilde{e}_\delta} \in \boldsymbol{Q}(\zeta_l). \tag{5}$$

Let π_0 be a prime element of $\boldsymbol{Q}_l(\zeta_l)$ such that $\pi_0^{l-1}=-l$ and $\zeta_l \equiv \operatorname{Exp} \pi_0 \pmod{\pi_0^l}$. Then $\pi_0^\sigma=\omega(\sigma)\pi_0$ for $\sigma \in G$, and $\pi \equiv \pi_0 \pmod{\pi^l}$. Since

$$e_\delta \pi_0^j=\begin{cases}\pi_0^j & \text{if } j=2i+1,\\ 0 & \text{otherwise,}\end{cases}$$

where $\delta=\omega^{2i+1}$ with $1 \leqq i \leqq (l-3)/2$, by Theorem 1 we have

$$g(\chi_\mathfrak{p}^{-1})^{\tilde{e}_\delta} \equiv 1-\beta_{2i}\frac{\pi_0^{2i+1}}{(2i+1)!} \pmod{\pi_0^l}. \tag{6}$$

Since $e_\delta \pi_0^l=0$, by making e_δ operate on both members of (6) we have

$$g(\chi_\mathfrak{p}^{-1})^{\tilde{e}_\delta} \equiv 1-\beta_{2i}\frac{\pi_0^{2i+1}}{(2i+1)!} \pmod{\pi_0^{l+1}}. \tag{7}$$

Since Y is a finite abelian l-group and $d \not\equiv 0 \pmod{l}$, by (4), (5) and (7) we see that $\mathrm{Cl}(\mathfrak{p}^{h'})^{e_\delta l^{m(\delta)}}=1$ in Y_δ if and only if $\beta_{2i} \equiv 0 \pmod{l}$, where $\mathrm{Cl}(\mathfrak{p}^{h'}) \in Y$ is the class containing $\mathfrak{p}^{h'}$. Since $\beta_{2i} \equiv 0 \pmod{l}$ if and only if $\mathfrak{p}$ is decomposed in $\boldsymbol{Q}(\zeta_l)(\sqrt[l]{\varepsilon_{2i}})/\boldsymbol{Q}(\zeta_l)$, we see by Čebotarev's density theorem that $\varepsilon_{2i} \in \boldsymbol{Q}(\zeta_l)^l$ if and only if $\beta_{2i} \equiv 0 \pmod{l}$ for all $\mathfrak{p} \in I$ (In this case,

Čebotarev's density theorem is proved purely algebraically by Wojcik [17]). Hence $\varepsilon_{2i} \in \boldsymbol{Q}(\zeta_l)^l$ if and only if $\mathrm{Cl}(\mathfrak{p}^{h'})^{e_\delta l^{m(\delta)}}=1$ for all $\mathfrak{p} \in I$. This gives the assertion.

§ 5. Relation between Iwasawa's formula on power residue symbols for the cyclotomic units and the congruence for Gauss sums

Iwasawa gives a highly interesting explicit formula on the l-th power residue symbol for cyclotomic units in $\boldsymbol{Q}(\zeta_l)$, by using Artin-Hasse's explicit formula on the norm residue symbol in local class field theory (Iwasawa [9], Lemma 1; see also Theorem 4 below). In this section, we shall give an elementary proof of Iwasawa's formula by using Theorem 1 for $n=1$.

Conversely, we shall give another proof of Theorem 1 (for $n=1$) by using Iwasawa's formula.

Definition. For any ideal $\mathfrak{a}$ of $\boldsymbol{Q}(\zeta_m)$ which is prime to m, put

$$G(\mathfrak{a})=\prod_{\mathfrak{p}} g(\chi_{\mathfrak{p}}^{-1})^{e_{\mathfrak{p}}},$$

where $\mathfrak{a}=\prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ is the prime ideal decomposition of $\mathfrak{a}$.

The link between Iwasawa's formula and the congruence for Gauss sums stated in Theorem 1 is the following Lemma 12 which is proved by using Stickelberger's theorem.

Lemma 12. *Let $n \geqq 1$ be any natural number and let l be any odd prime number. Let $\mathfrak{a}$ be any ideal of $\boldsymbol{Q}(\zeta_{l^n})$ which is prime to l and let $\alpha \in \boldsymbol{Q}(\zeta_{l^n})$ be such that $\mathfrak{a}^{l^t}=(\alpha)$ with $t \geqq 0$. Let δ be any Dirichlet character defined modulo l^n and put*

$$\tilde{M}(\delta)=\sum_{a=1}^{l^i} a\delta(a),$$

where l^i is the conductor of δ. Put

$$\xi=\sum_{\substack{a=1 \\ (a,l)=1}}^{l^n} a\sigma_a^{-1} \in \boldsymbol{Z}[G],$$

where $G=G(\boldsymbol{Q}(\zeta_{l^n})/\boldsymbol{Q})$. Then

$$\log G(\mathfrak{a})=\frac{1}{l^{n+t}}\xi \log \alpha$$

and

$$e_\delta \log G(\mathfrak{a}) = \frac{1}{l^{t+t}} \tilde{M}(\delta^{-1})(e_\delta \log \alpha),$$

where log *is the l-adic* log.

Proof. By Stickelberger's theorem,

$$(g(\chi_\mathfrak{p}^{-1})^{l^n}) = \mathfrak{p}^\xi,$$

so

$$(G(\mathfrak{a})^{l^n}) = \mathfrak{a}^\xi. \tag{1}$$

Note that $G(\mathfrak{a})^{l^n} \in \boldsymbol{Q}(\zeta_{l^n})$. Since

$$\xi(1+\sigma_{-1}) = l^n \sum_{t \in (\boldsymbol{Z}/l^n)^\times} \sigma_t,$$

by making $(1+\sigma_{-1})$ operate on the both members of (1) we have

$$(G(\mathfrak{a})^{l^n})^{1+\sigma_{-1}} = (N\mathfrak{a})^{l^n} \tag{2}$$

as numbers. On the other hand, by taking the l^t-th power of the both members of (1) we have

$$(G(\mathfrak{a})^{l^{n+t}}) = (\mathfrak{a}^{l^t})^\xi$$

as ideals, so

$$(G(\mathfrak{a})^{l^{n+t}}) = (\alpha^\xi)$$

as ideals. Hence

$$G(\mathfrak{a})^{l^{n+t}} = e\alpha^\xi \tag{3}$$

with some unit e in $\boldsymbol{Q}(\zeta_{l^n})$. By making $(1+\sigma_{-1})$ operate on both members of (3), we have

$$(G(\mathfrak{a})^{l^{n+t}})^{1+\sigma_{-1}} = e^{1+\sigma_{-1}}(N_{\boldsymbol{Q}(\zeta_{l^n})/\boldsymbol{Q}}(\alpha))^{l^n}. \tag{4}$$

Since $\boldsymbol{Q}(\zeta_{l^n})$ is totally imaginary, by taking $N_{\boldsymbol{Q}(\zeta_{l^n})/\boldsymbol{Q}}$ of the equality $\mathfrak{a}^{l^t} = (\alpha)$ we have

$$(N\mathfrak{a})^{l^t} = N_{\boldsymbol{Q}(\zeta_{l^n})/\boldsymbol{Q}}(\alpha). \tag{5}$$

By (2), (4) and (5) we have $e^{1+\sigma_{-1}} = 1$, so e is a root of unity in $\boldsymbol{Q}(\zeta_{l^n})$. Since $\log e = 0$, by taking log of both members of (3) we have

$$l^{n+t} \log G(\mathfrak{a}) = \xi \log \alpha. \tag{6}$$

Note that

$$e_\delta(\xi \log \alpha)=(e_\delta \xi)\log \alpha, \tag{7}$$

since $\xi \in Z[G]$. Since

$$e_\delta \xi=\left(\sum_{a=1}^{l^n} a\delta^{-1}(a)\right)e_\delta$$

and

$$\sum_{a=1}^{l^n} a\delta^{-1}(a)=l^{n-t}\tilde{M}(\delta^{-1})$$

by elementary computation, by making e_δ operate on both members of (6) and using (7), we have

$$l^{n+t}e_\delta \log G(\mathfrak{a})=l^{n-t}\tilde{M}(\delta^{-1})e_\delta \log \alpha,$$

so we have the assertion.

Remark. We can get a similar formula for Jacobi sums as the formula in Lemma 12, by using Lemmas 4 and 12.

Now assume $l \geqq 5$. For any odd Dirichlet character δ defined modulo l such that $\delta \neq \omega$, let ε_δ be the cyclotomic unit of $\boldsymbol{Q}(\zeta_l)$ defined in Section 1, where $\hat{\delta}=\omega\delta^{-1}$. For any ideal $\mathfrak{a}$ of $\boldsymbol{Q}(\zeta_l)$ which is prime to l, let

$$[\varepsilon_\delta, \mathfrak{a}]=[\varepsilon_\delta, \mathfrak{a}]_l$$

be as in Section 1. Then Iwasawa ([9], Lemma 1) gives an explicit formula of $[\varepsilon_\delta, \mathfrak{a}]$ as follows.

Theorem 4 (Iwasawa). *Let the notation and assumptions be as above. Suppose that* $\mathfrak{a}^{l^t}=(\alpha)$ *with* $\alpha \in \boldsymbol{Q}(\zeta_l)$ *and* $t \geqq 0$. *Then*

$$[\varepsilon_\delta, \mathfrak{a}] \equiv \frac{1}{l^{t+1}} M(\delta^{-1})u_\delta \qquad (\mathrm{mod}\ l\boldsymbol{Z}_l),$$

where $M(\delta^{-1})$ *is as in Lemma 5 and* $u_\delta \in \boldsymbol{Q}_l$ *is such that*

$$e_\delta(\log \alpha)=u_\delta \gamma_\delta \text{ with } \gamma_\delta=\frac{1}{l-1}\sum_{a=1}^{l-1}\delta(a)^{-1}\zeta_l^a.$$

Remark. Iwasawa [9] assumes that $\alpha \equiv 1 \pmod{\pi}$, but this assumption can be omitted, by using the equalities $(\alpha^{l-1})^{l^t}=\alpha^{l-1}$ and $\log \alpha^{l-1}=(l-1)\log \alpha$.

Lemma 13. *Let $\mathfrak{a}$ be any ideal of $\boldsymbol{Q}(\zeta_l)$ which is prime to l and let π be a prime element of $\boldsymbol{Q}_l(\zeta_l)$ as in Section 1. Write*

$$G(\mathfrak{a}) \equiv \mathrm{Exp}\left(\sum_{j=1}^{l-1} \lambda_j \frac{\pi^j}{j!}\right) \pmod{\pi^l}$$

with $\lambda_j \in \boldsymbol{Z}_l[\zeta_p]$ $(j=1, \cdots, l-1)$. Let $\alpha \in \boldsymbol{Q}(\zeta_l)$ be such that $\mathfrak{a}^{l^t}=(\alpha)$ with $t \geqq 0$. Put $\delta=\omega^j$ with $2 \leqq j \leqq l-2$. Let $u_\delta \in \boldsymbol{Q}_l$ be such that $e_\delta \log \alpha = u_\delta \gamma_\delta$, where γ_δ is as in Theorem 4, and let $M(\delta^{-1})$ be as in Lemma 5. Then

$$\lambda_j \equiv \frac{1}{l^{t+1}} M(\delta^{-1}) u_\delta \pmod{l\boldsymbol{Z}_l}.$$

In particular, we have $\lambda_j \equiv 0 \pmod{l\boldsymbol{Z}_l}$ if j is even.

Proof. Lemma 12 is essential for our proof. Since

$$\sigma_a \pi \equiv \omega(a)\pi \pmod{\pi^l}$$

for $a \not\equiv 0 \pmod{l}$, we have

$$e_\delta \pi^i \equiv \begin{cases} \pi^i & \pmod{\pi^l} \quad \text{if } j=i, \\ 0 & \pmod{\pi^l} \quad \text{otherwise,} \end{cases} \tag{1}$$

for $0 \leqq i \leqq l-1$. Since $\gamma_\delta = e_\delta(\zeta_l)$ by definition and $\zeta_l \equiv \mathrm{Exp}\,\pi \pmod{\pi^l}$, we have

$$\gamma_\delta \equiv \frac{1}{j!}\pi^j \pmod{\pi^l}. \tag{2}$$

By (1) we have

$$G(\mathfrak{a})^{e_\delta} \equiv \mathrm{Exp}\left(\lambda_j \frac{\pi_j}{j!}\right) \pmod{\pi^l}.$$

Taking log of the both members, we have

$$e_\delta \log G(\mathfrak{a}) \equiv \lambda_j \frac{\pi^j}{j!} \pmod{\pi^{j+1}}. \tag{3}$$

On the other hand, by Lemma 12 we have

$$e_\delta \log G(\mathfrak{a}) = \frac{1}{l^{t+1}} M(\delta^{-1}) u_\delta \gamma_\delta. \tag{4}$$

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

$$\lambda_j \equiv \frac{1}{l^{t+1}} M(\delta^{-1}) u_\delta \qquad (\mathrm{mod}\, l\boldsymbol{Z}_l),$$

since $\lambda_j \in \boldsymbol{Z}_l[\zeta_p]$ and $M(\delta^{-1}) \in \boldsymbol{Z}_l$. Since $M(\delta^{-1})=0$ if j is even, the last assertion follows from this.

Another proof of Theorem 4. Write $\delta=\omega^{2i+1}$ with $1 \leqq i \leqq (l-3)/2$. By Lemma 13,

$$\lambda_{2i+1} \equiv \frac{1}{l^{t+1}} M(\delta^{-1}) u_\delta \qquad (\mathrm{mod}\, l\boldsymbol{Z}_l). \tag{1}$$

On the other hand, by using Theorem 1 for $a=-1$ we have

$$\lambda_{2i+1} \equiv [\varepsilon_\delta, \mathfrak{a}] \qquad (\mathrm{mod}\, l\boldsymbol{Z}_l). \tag{2}$$

By (1) and (2) we have the assertion.

Another proof of Theorem 1 *when* $n=1$. We may assume $a=-1$. Write $g(\chi_\mathfrak{p}^{-1})$ as in Lemma 13 for $\mathfrak{a}=\mathfrak{p}$. By Lemma 13, $\lambda_j \equiv 0 \pmod{l\boldsymbol{Z}_l}$ if j is even. By Theorem 4 and Lemma 13, we have

$$\lambda_{2i+1} \equiv -\beta_{2i+1} \qquad (\mathrm{mod}\, l) \qquad \text{for } 1 \leqq i \leqq \frac{l-3}{2}.$$

Since

$$g(\chi_\mathfrak{p}^{-1}) = -\sum_{x \in \boldsymbol{F}_q^\times} \zeta_l^{-\lambda(x)} \psi(x)$$

by definition and since $\zeta_l \equiv 1+\pi \pmod{\pi^2}$, we have

$$g(\chi_\mathfrak{p}^{-1}) \equiv 1-\alpha_1\pi \qquad (\mathrm{mod}\, \pi^2).$$

Since $g(\chi_\mathfrak{p}^{-1})^{1+\sigma-1} = \pm q$ and since $g(\chi_\mathfrak{p}^{-1}) \equiv 1 \pmod{\pi}$, we have

$$g(\chi_\mathfrak{p}^{-1})^{e_1} = q^{1/2}. \tag{1}$$

Since

$$e_1\pi^j \equiv \begin{cases} \pi^j & (\mathrm{mod}\, \pi^l) \quad \text{if } j=l-1, \\ 0 & (\mathrm{mod}\, \pi^l) \quad \text{otherwise,} \end{cases}$$

for $1 \leqq j \leqq l-1$, by (1) we have

$$\mathrm{Exp}\left(\frac{\lambda_{l-1}}{(l-1)!}\pi^{l-1}\right) \equiv q^{1/2} \qquad (\mathrm{mod}\, \pi^l),$$

so

$$\lambda_{l-1} l \equiv \frac{1}{2} \operatorname{Log} q \qquad (\mathrm{mod}\ \pi^l),$$

since $(l-1)! \equiv -1 \pmod{l}$ and $\pi^{l-1} \equiv -l \pmod{\pi^l}$. Hence

$$\lambda_{l-1} \equiv \frac{q-1}{2l} \qquad (\mathrm{mod}\ l).$$

References

[1] G. W. Anderson, The hyperadelic gamma function, this volume, 1–19.
[2] R. F. Coleman, "Applications" of Ihara's power series to cyclotomic fields, a lecture at Univ. Tokyo in Oct. 1985.
[3] P. Deligne, Applications de la formule des traces aux sommes trigonométriques, Sém. Géom. Alg. SGA 4 1/2, Cohomologie Etale, Lecture Notes in Math., **569**, pp. 168–232, Springer, Berlin Heidelberg New York 1977.
[4] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.
[5] Y. Ihara, Profinite braid groups, Galois representations and complex multiplications, Ann. of Math., **123** (1986), 43–106.
[6] Y. Ihara, M. Kaneko and A. Yukinari, On some properties of the universal power series for Jacobi sums, this volume, 65–86.
[7] K. Iwasawa, Lectures on p-adic L-functions, Ann. of Math. Studies, No. 74, Princeton, 1972.
[8] ——, A note on Jacobi sums, Symposia Math., **15** (1975), 447–459.
[9] ——, A note on cyclotomic fields, Invent. Math., **36** (1976), 115–123.
[10] T. Metsänkylä, A short proof of the nonvanishing of a character sum, J. Number Theory, **9** (1977), 507–509.
[11] T. Uehara, On cyclotomic units connected with p-adic characters, J. Math. Soc. Japan, **37** (1985), 65–77.
[12] S. Ullom, The nonvanishing of certain character sums, Proc. Amer. Math. Soc., **45** (1974), 164–166.
[13] L. C. Washington, Introduction to cyclotomic fields, Springer, New York Heidelberg Berlin, 1980.
[14] A. Weil, Number of solutions of equations in finite fields, Bull. Amer. Math. Soc., **55** (1949), 497–508.
[15] ——, Jacobi sums as "Grossencharaktere", Trans. Amer. Math. Soc., **73** (1952), 487–495
[16] ——, Basic Number Theory, 3rd ed. Springer, New York, 1974.
[17] J. Wojcik, A purely algebraic proof of special cases of Tchebotarev's theorem, Acta Arith., **28** (1975), 137–145.

Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Setagaya-ku, Tokyo 158
Japan