J. Math. Soc. Japan
Vol. 48, No. 2, 1996

Jacobi sums and the Hilbert symbol for a power of two(*)

By Hiroo MIKI

(Received Sept. 9, 1992)
(Revised Aug. 22, 1994)

Many number theorists have taken up the problem of determining the exact conductor $C_m^{(a)}$ of the Jacobi sum Hecke character $\mathfrak{a}\mapsto J_m^{(a)}(\mathfrak{a})$ since Weil [**18**] raised its interesting problem in 1952. Recently, Coleman-McCallum [**2**] determined the exact conductor $C_m^{(a)}$ when m is a power of any *odd* prime number l, using the arithmetic geometry of Fermat curves, and Miki [**12**], [**13**], [**14**] gave a purely number theoretic proof to their results. But the case $l=2$ is still an unsolved more difficult open problem, and it seems that Coleman-McCallum's method [**2**] is not applicable to the case $l=2$, though Coleman [**3**], § 6 (with G. Anderson) gave a partial result by using Ihara-Anderson's theory.

The purpose of the present paper is to give the complete determination of the conductor $f_n(g, h, s)$ of the character $\alpha\mapsto(\alpha, 2^g(1+4)^h(-1)^s)_n$ with $g\in\boldsymbol{Z}$, $h\in\boldsymbol{Z}_2$, and $s\in\boldsymbol{Z}/2\boldsymbol{Z}$ for $n\geqq 2$ (see Theorem 5 in § 1), and the conductor $C_{2^n}^{(a)}$ of the Jacobi sum Hecke character $\mathfrak{a}\mapsto J_{2^n}^{(a)}(\mathfrak{a})$ for the power 2^n (see Corollary to Theorem 9 in § 2), by the methods of [**13**], [**14**]. Here, $\boldsymbol{Z}$ and $\boldsymbol{Z}_2$ are the rings of rational and 2-adic integers respectively, and $(\ ,\ )_n$ denotes the Hilbert norm residue symbol in $\boldsymbol{Q}_2(\zeta_{2^n})$ for the power 2^n, where $\boldsymbol{Q}_2$ is the field of 2-adic numbers and ζ_{2^i} is a fixed primitive 2^i-th root of unity satisfying $\zeta_{2^{i+1}}^2=\zeta_{2^i}$ for all $i\geqq 1$ (for the exact definition, see [**14**], § 1).

Since $\delta^{(n)}(\alpha)$ is well-defined mod 2^{n-1} (not mod 2^n) when $l=2$ (see Lemma 6 in § 2), we can determine $i_{2^n}^{(a)}(\alpha)$ mod 2^{n-1} in the same way as [**13**] (see Theorem 8 in § 2). In Theorem 9 (see also its Remark) in § 2, we will determine $i_{2^n}^{(a)}(\alpha)$ mod 2^n for $\alpha\in\boldsymbol{Q}(\zeta_{2^n})$, $\alpha\equiv 1\ (\mathrm{mod}\ \pi_n^3)$, by using Theorem 8 and certain congruences for Jacobi sums (see Theorems 12, 13, and 14 in § 3). Note that Theorem 9 (and its Remark) contains Coleman [**3**], Theorem (6.4) as a special case. Theorem 9, combined with Theorem 5, gives the complete determination of the conductor $C_{2^n}^{(a)}$ (see Corollary to Theorem 9).

(*) This paper contains the details of part of my talk at the Number Theory Seminar (Goldfeld), Columbia Univ., March 21, 1988 (see [**12**]).

§ 1. Conductor of the character $\alpha\mapsto(\alpha, 2^g(1+4)^h(-1)^s)_n$.

In this section, we retain all the notations in [**14**] putting $l=2$, and assume $n\geqq 2$. For example, T_n is the trace from $\boldsymbol{Q}_2(\zeta_{2^n})$ to $\boldsymbol{Q}_2$, $\pi_n=1-\zeta_{2^n}$, and

$$\xi_a=\exp\Big(-\sum_{\substack{i=1\\2\nmid i}}^{\infty}\frac{(\pi_n^a)^i}{i}\Big)\quad\text{for } a>2^{n-1},$$

where exp is the 2-adic exponential function.

LEMMA 1. *If* $a\geqq 1$, *then*

$$T_n(a\zeta_{2^n}\pi_n^{a-1})\equiv 0 \pmod{2^{2n-2}}.$$

PROOF. Since

$$(*)\qquad T_n(\zeta_{2^n}^i)=\begin{cases}0 & \text{if } 2^{n-1}\nmid i,\\ 2^{n-1}\zeta_{2^n}^i & \text{if } 2^{n-1}\mid i,\end{cases}$$

and

$$\begin{aligned}a\zeta_{2^n}\pi_n^{a-1}&=a\zeta_{2^n}\sum_{i=0}^{a-1}(-1)^i\binom{a-1}{i}\zeta_{2^n}^i\\&=-\sum_{i=0}^{a}(-1)^i i\binom{a}{i}\zeta_{2^n}^i,\end{aligned}$$

we have

$$\begin{aligned}T_n(a\zeta_{2^n}\pi_n^{a-1})&=-2^{2n-2}\sum_{0\leqq 2^{n-1}k\leqq a}k\binom{a}{2^{n-1}k}(-1)^k\\&\equiv 0 \pmod{2^{2n-2}}.\end{aligned}$$

LEMMA 2. *If* $a>2^{n-1}$, *then the following* (i), (ii) *and* (iii) *hold.*

(i) $\delta_n(\xi_a)\equiv-\sum_{\substack{i=1\\(i,2)=1}}^{\infty}a\zeta_{2^n}\pi_n^{a\,i-1} \pmod{D_n}$, *where* $D_n=(2^{n-1})$ *is the different of* $\boldsymbol{Q}_2(\zeta_{2^n})/\boldsymbol{Q}_2$.

(ii) $T_n(\delta_n(\xi_a))\equiv 0 \pmod{2^{2n-2}}$ *for* $a>2^{n-1}$.

(iii) *If* $\alpha\equiv 1 \pmod 2$ *and* $\alpha\in\boldsymbol{Q}_2(\zeta_{2^n})$, *then* $T_n(\delta_n(\alpha))\equiv 0 \pmod{2^{2n-2}}$.

PROOF. (i) The proof is almost the same as that of [**14**], Lemma 7, (i). In fact, we can replace (2), (5), and (6) in the proof by the following (2)′, (5)′, and (6)′, respectively:

(2)′ $\qquad f(\pi_n)=\beta-1$ and $f(T)\equiv T^b \pmod{T^{b+1}}$.

(5)′ $\qquad u(\pi_n)\equiv 0 \pmod 2$.

(6)′ $\qquad \delta_n(\beta)\equiv-\zeta_{2^n}\dfrac{a\pi_n^{2a-1}}{1-\pi_n^{2a}} \pmod{D_n}$.

Hence we have the assertion.

(ii) Since $T_n(D_n)\equiv 0 \pmod{2^{2n-2}}$, by (i) we have

$$T_n(\delta_n(\xi_a)) \equiv -\sum_{\substack{i=1\\(i,2)=1}}^{\infty} \frac{1}{i} T_n((ai)\zeta_{2^n}\pi_n^{ai-1}) \pmod{2^{2n-2}}.$$

Hence, by Lemma 1 we have the assertion.

(iii) If $\alpha\equiv 1 \pmod 2$ and $\alpha\in \boldsymbol{Q}_2(\zeta_{2^n})$, then we can write

$$\alpha = \prod_{a\geq 2^{n-1}} \xi_a^{\lambda_a} \quad \text{with } \lambda_a \in \boldsymbol{Z},$$

where $\xi_{2^{n-1}}=1-2=-1$. Since $\delta_n(-1)\equiv 0 \pmod{D_n}$, by (ii) and Iwasawa [7], Lemma 4, i) we have the assertion.

THEOREM 1.

$$f_n(0, 2^i, 0) = \begin{cases} (\pi_{i+1}) & \textit{for } 0 \leqq i \leqq n-2, \\ (1) & \textit{for } i \geqq n-1. \end{cases}$$

PROOF. Since Iwasawa [7], Theorem 2 is valid for $l=2$ by Kudo [9], we have

$$(1) \qquad [\alpha, 1+4]_n \equiv -\frac{1}{2^n} T_n(\delta_n(\alpha)\log(1+4)) \pmod{2^n}$$

$$\equiv -\frac{1}{2^n}\log(1+4) T_n(\delta_n(\alpha)) \pmod{2^n}$$

for $\alpha\in \boldsymbol{Q}_2(\zeta_{2^n})^\times$. Since $\log(1+4)\equiv 4 \pmod 8$, by Lemma 2, (iii) we see that

$$(2) \qquad [\alpha, 1+4]_n \equiv 0 \pmod{2^n} \quad \text{if } \alpha \equiv 1 \pmod 2.$$

Next, we will show

$$(3) \qquad [1+2\pi_n^{-1}, 1+4]_n \not\equiv 0 \pmod{2^n}.$$

If $\sigma(\neq 1)\in \mathrm{Gal}(\boldsymbol{Q}_2(\zeta_{2^n})/\boldsymbol{Q}_2(\zeta_{2^{n-1}}))$, then $\zeta_{2^n}^\sigma = -\zeta_{2^n} = \zeta_{2^n}^{1+2^{n-1}}$ and $\pi_n^{\sigma-1} = -1+2\pi_n^{-1} \equiv 1+2\pi_n^{-1} \pmod 2$. Hence by (2),

$$\begin{aligned}(1+2\pi_n^{-1}, 1+4)_n &= (\pi_n^{\sigma-1}, 1+4)_n \\ &= (\pi_n, 1+4)_n^{2^{n-1}} \\ &= (\pi_n, 1+4)_n',\end{aligned}$$

where $(\ ,\ )_n'$ denotes the quadratic Hilbert symbol in $\boldsymbol{Q}_2(\zeta_{2^n})$. Since $\boldsymbol{Q}_2(\zeta_{2^n})(\sqrt{1+4})/\boldsymbol{Q}_2(\zeta_{2^n})$ is unramified of degree 2, by local class field theory we have

$$(\pi_n, 1+4)_n' \neq 1,$$

hence we have (3). (Alternatively, $(\pi_n, 1+4)_n' = (N_n(\pi_n), 1+4)_1 = (2, 1+4)_1 \neq 1$ by e.g., Serre [16], Chap. XIV, § 4). By (2) and (3), $f_n(0, 1, 0) = (\pi_1) = (2)$. Hence,

by [14], Lemma 12, we have $f_n(0, 2^i, 0)=(\pi_{i+1})$ for $0\leqq i\leqq n-2$. Since $T_n(\boldsymbol{Z}_2[\zeta_{2^n}])\equiv 0 \pmod{2^{n-1}}$, we see by (1) that $[\alpha, 1+4]_n\equiv 0 \pmod 2$ if $\alpha\equiv 1\ (\pi_n)$. Hence $f_n(0, 2^i, 0)=(1)$ for $i\geqq n-1$.

REMARK. The direct calculation using the above (1) shows also $[\pi_n, 1+4]_n \not\equiv 0 \pmod 2$.

For positive integers c and i such that $n\geqq i+1$, put

$$r_n^{(i)}(c)=\sum_{0\leqq 2^{n-i}k\leqq c}\binom{c}{2^{n-i}k}\zeta_{2^i}^k\in \boldsymbol{Z}[\zeta_{2^i}].$$

LEMMA 3. *Under the above notation and assumptions, the following* (i)$\sim$(v) *hold.*

(i) *If* $n\geqq i+1$, *then* $r_{n+1}^{(i)}(2c)\equiv r_n^{(i)}(c) \pmod 4$.

(ii) *If* $n\geqq i+1$, *then* $r_{n+1}^{(i)}(c)\equiv r_{n+1}^{(i)}(c-1) \pmod 4$ *for any odd* $c\geqq 3$.

(iii) $r_2^{(1)}(2)=0$, $r_2^{(1)}(3)\equiv 2 \pmod 4$, *and* $r_3^{(2)}(5)\equiv \pi_2^2 \pmod 4$.

(iv) *If* $n\geqq 2$, *then* $r_n^{(1)}(c)\equiv\begin{cases} 0 \pmod 4 & \text{for } 2^{n-1}\leqq c<2^{n-1}+2^{n-2},\\ 2 \pmod 2 & \text{for } 2^{n-1}+2^{n-2}\leqq c<2^n.\end{cases}$

(v) *If* $n\geqq 3$, *then* $r_n^{(2)}(c)\equiv \pi_2^2 \pmod 4$ *for* $c=2^{n-1}+2^{n-2}-1$.

PROOF. (i) By Artin-Hasse [1], Hilfssatz 2,

$$\binom{2c}{2^{n+1-i}k}\equiv\binom{c}{2^{n-i}k} \pmod 4,$$

since $n\geqq i+1$. By this we immediately have the assertion.

(ii) Since $n\geqq i+1$ and c is odd,

$$\binom{c}{2^{n+1-i}k}=\frac{c}{c-2^{n+1-i}k}\binom{c-1}{2^{n+1-i}k}\equiv\binom{c-1}{2^{n+1-i}k} \pmod 4.$$

On the other hand, $0\leqq 2^{n+1-i}k\leqq c$ if and only if $0\leqq 2^{n+1-i}k\leqq c-1$. This gives the assertion.

(iii) $r_2^{(1)}(3)=1-3=-2$, and $r_3^{(2)}(5)=-4+10\zeta_4\equiv\pi_2^2 \pmod 4$.

(iv) We will prove it by induction on n. If $n=2$, then $c=2, 3$, so the assertion follows from (iii). Now assume $n\geqq 3$. Write $c=c_0+2c_1$ with $c_0, c_1\in\boldsymbol{Z}$, $0\leqq c_0<2$. Then the inequalities of the assumption imply

$$2^{n-2}\leqq c_1<2^{n-2}+2^{n-3}$$

and

$$2^{n-2}+2^{n-3}\leqq c_1<2^{n-1},$$

respectively. By (i) and (ii), we have

$$r_n^{(1)}(c)\equiv r_n^{(1)}(c-c_0)=r_n^{(1)}(2c_1)\equiv r_{n-1}^{(1)}(c_1) \pmod 4.$$

Hence the assertion follows from the induction hypothesis.

(v) We can prove it in the same way as the proof of (iv).

LEMMA 4. *The following* (i) *and* (ii) *hold.*

(i) $\frac{1}{2^{n-1}}T_n(\pi_n^c)\equiv\begin{cases}0 \pmod 4 & \text{if } 2^{n-1}\leqq c<2^{n-1}+2^{n-2},\\ 2 \pmod 4 & \text{if } 2^{n-1}+2^{n-2}\leqq c<2^n.\end{cases}$

(ii) $\frac{1}{2^{n-2}}T_{n,2}(\pi_n^c)\equiv\pi_2^2 \pmod 4$ *if* $c=2^{n-1}+2^{n-2}-1$.

PROOF. (i) By (*) in the proof of Lemma 1, we have easily $T_n(\pi_n^c)=2^{n-1}r_n^{(1)}(c)$. Hence the assertion follows from Lemma 3, (iv).

(ii) This follows from Lemma 3, (v) in the same way as the proof of (i).

THEOREM 2.

(i) $[\xi_a, 2^2]_n\equiv\begin{cases}2^{n-1} \pmod{2^n} & \text{if } 2^{n-1}+2^{n-2}\leqq a<2^n\\ & \text{or if } a=2^{n-1}+2^{n-2}-1 \text{ and } n\geqq 3,\\ 0 \pmod{2^n} & \text{if } a\geqq 2^n.\end{cases}$

(ii) $[\xi_a, -1]_n\equiv\begin{cases}2^{n-1} \pmod{2^n} & \text{if } 2^{n-1}+2^{n-2}\leqq a<2^n,\\ 0 \pmod{2^n} & \text{if } 2^{n-1}<a<2^{n-1}+2^{n-2} \text{ or if } a\geqq 2^n.\end{cases}$

PROOF. (i) If $a\geqq 2^n$, then the proof of [**14**], Theorem 2 is valid for $l=2$, since [**14**], Lemma 9, (i) (iii) are valid for $l=2$. If $2^{n-1}+2^{n-2}\leqq a<2^n$, then the equality (3) (for $i=1$) in the proof of [**14**], Theorem 2 is valid for $l=2$ by using Lemma 4, (i) in place of [**14**], Lemma 9, (ii). Hence

$$\begin{aligned}(\xi_a, 2^2)_n &= (\exp(-4), 2)_1\\ &= (1-4, 2)_1\end{aligned}$$

for $2^{n-1}+2^{n-2}\leqq a<2^n$. Hence $(\xi_a, 2^2)_n=-1$. This gives the first congruence. If $a=2^{n-1}+2^{n-2}-1$ and $n\geqq 3$, then the equality (3) in the proof of [**14**], Theorem 2 holds for $i=2$ by using Lemma 4, (ii) in place of [**14**], Lemma 9, (ii). Hence

$$\begin{aligned}(\xi_a, 2^2)_n &= (\exp(-2\pi_2^2), 2)_2\\ &= (\exp(-2\pi_2^2), \zeta_4)_2(\exp(-2\pi_2^2), \pi_2)_2^2,\end{aligned}$$

since $2=\zeta_4\pi_2^2$. By Artin-Hasse's explicit formula [**1**],

$$(\exp(-2\pi_2^2), \zeta_4)_2 = 1 \quad \text{and} \quad (\exp(-2\pi_2^2), \pi_2)_2^2 = -1,$$

since $T_2(\pi_2^2)=0$. So $(\xi_a, 2^2)_n=-1$. This gives the first congruence.

(ii) Assume $a\geqq 2^{n-1}$. By Artin-Hasse's explicit formula [**1**],

$$[\xi_a, -1]_n = -2^{n-1}[\zeta_{2^n}, \xi_a]_n$$
$$\equiv -2^{-1}(1+2^{n-1})T_n(\log \xi_a) \pmod{2^n}$$
$$\equiv 2^{-1}T_n\Big(\sum_{\substack{i=1\\(i,2)=1}}^{\infty} \frac{\pi_n^{ai}}{i}\Big) \pmod{2^n}.$$

Hence by [**14**], Lemma 9, (iii),

$$[\xi_a, -1]_n \equiv 2^{-1}T_n(\pi_n^a) \pmod{2^n},$$

since $ai \geqq 2^n$ for $i \geqq 2$. Hence by Lemma 4, (i), we have the assertion.

COROLLARY.

(i) $f_n(2, 0, 0)=f_n(0, 0, 1)=(4)$.

(ii) $f_n(2, 0, 1)=\begin{cases} (\pi_1\pi_2) & \text{if } n \geqq 3, \\ (1) & \text{if } n=2. \end{cases}$

ANOTHER PROOF. (i) Cf. The proof of Corollary to Theorem 3.

(ii) Since $-2^2=\pi_2^4$, we have $\boldsymbol{Q}_2(\zeta_{2^n})(\sqrt[2^n]{-2^2})=\boldsymbol{Q}_2(\zeta_{2^n})(\sqrt[2^{n-2}]{\pi_2})$. The case $n=2$ is trivial, so we assume $n \geqq 3$. By the following Theorem 3, the last upper ramification number of $\boldsymbol{Q}_2(\zeta_{2^n})(\sqrt[2^n]{-2^2})/\boldsymbol{Q}_2(\zeta_{2^n})$ is $3\cdot 2^{n-2}-1$. Hence by the conductor-ramification theorem, $f_n(2, 0, 1)=(\pi_n^{3\cdot 2^{n-2}})=(\pi_2^3)=(\pi_1\pi_2)$.

We will determine the conductor $f_n(2^i, 0, 0)$ for $i \geqq 2$ by using ramification theory. (For the proof using (ii) of the above corollary and [**14**], Lemma 12, see another proof of Corollary to Theorem 3.)

THEOREM 3. *Put $k_n=\boldsymbol{Q}_2(\zeta_{2^n})$. Let π be any prime element of k_2. Then $k_n(\sqrt[2^n]{\pi})/k_n$ is a fully ramified cyclic extension of degree 2^n with upper ramification numbers r_i $(1 \leqq i \leqq n)$:*

$$r_i = 2^{i+1}+2^i-1 = 3\cdot 2^i-1 \quad \text{for } 1 \leqq i \leqq n-2,$$
$$r_{n-1} = 2^n+2^{n-2}-1 = 5\cdot 2^{n-2}-1,$$

and

$$r_n = 2^n+2^{n-1}+2^{n-2}-1 = 7\cdot 2^{n-2}-1.$$

PROOF. Put $K_m=k_2(\sqrt[2^m]{\pi})$, $L_m=k_n(\sqrt[2^m]{\pi})$ for $0 \leqq m \leqq n$, $K=K_0$, and $L=L_0$. (Take $\sqrt[2^m]{\pi}$ so that $(\sqrt[2^m]{\pi})=\sqrt[2^{m-1}]{\pi}$ for $1 \leqq m \leqq n$.) We define the Hasse function $\psi_{K_m/K}$ by

$$\psi_{K_m/K} = \psi_{K_m/K_{m-1}} \circ \cdots \circ \psi_{K_2/K_1} \circ \psi_{K_1/K},$$

where $\psi_{K_i/K_{i-1}}$ is the Hasse function of K_i/K_{i-1}. Then we see easily

(1) $$\psi_{L_m/K_m} \circ \psi_{K_m/K} = \psi_{L_m/L} \circ \psi_{L/K}$$

by using induction on m and the transitivity of the Hasse function. As is well-known, the ramification numbers of L/K are $(2^{i+1}-1)$ with $i=1, 2, \cdots, n-2$, so the set of upper ramification numbers of L/K is

$$T_1 = \{2i+1 \mid i=1, 2, \cdots, n-2\}.$$

K_m/K_{m-1} is a fully ramified cyclic extension of degree 2 and $\sqrt[2^m]{\pi}$ is a prime element of K_m. Since $(\sqrt[2^m]{\pi})^{\tau-1}=-1=1-2$ for $\tau(\neq 1)\in \mathrm{Gal}(K_m/K_{m-1})$, the ramification number of K_m/K_{m-1} is 2^{m+1}. Hence the set of x-coordinates of points where the graph of $y=\phi_{K_n/K}(x)$ bends is

$$T_2 = \{2i+2 \mid i=1, 2, \cdots, n\}.$$

By (1) we see that the graph $y=\phi_{L_n/L}(x)$ bends at any point with x-coordinate in $\phi_{L/K}(T_2)$. Thus L_n/L is a fully ramified cyclic extension of degree 2^n with upper ramification numbers $\phi_{L/K}(2i+2)$ with $i=1, 2, \cdots, n$. For $1\leqq i\leqq n-2$,

$$\begin{aligned}\phi_{L/K}(2i+2) &= \phi_{L/K}(2i+1)+2^i \\ &= 2^{i+1}-1+2^i \\ &= 3\cdot 2^i-1.\end{aligned}$$

For $i=n-1, n$,

$$\begin{aligned}\phi_{L/K}(2i+2) &= \phi_{L/K}(2n-3)+2^{n-2}\{2(i-n)+5\} \\ &= 2^{n-1}-1+2^{n-2}\{2(i-n)+5\}.\end{aligned}$$

Thus we have the assertion.

REMARK. The above situation is a special case where Maus' general theory [**10**] can be applied, but in the above proof we gave a direct proof using only classical ramification theory found in e.g., Serre [**16**], Chap. IV.

COROLLARY.

$$f_n(2^i, 0, 0) = \begin{cases} (8) & \text{for } i=0, \\ (4) & \text{for } i=1, \\ (\pi_i\pi_{i+1}) & \text{for } 2\leqq i\leqq n-2, \\ (1) & \text{for } i\geqq n-1,\ i\neq 1. \end{cases}$$

PROOF. The first case follows from the second one, since the second power homomorphism of $U_n^{(m)}$ to $U_n^{(m+2^{n-1})}$ is the isomorphism for $m>2^{n-1}$ (e.g., Serre [**16**], Chap. XIV, § 4, Proposition 9). First, suppose $2\leqq i\leqq n-2$. By the conductor-ramification theorem (e.g., Serre [**16**], Chap. XV, § 2, Corollary to Theorem 1),

$$f_n(2^i, 0, 0) = (\pi_n^{r+1}),$$

where r is the last upper ramification number of $k_n(\sqrt[2^{n-i}]{2})/k_n$. Since

$$2=\zeta_{2^n}^{2^{n-2}}\pi_2^2,$$

we have

$$k_n(\sqrt[2^{n-i}]{2})=k_n(\sqrt[2^{n-i-1}]{\pi_2}).$$

Hence by Theorem 3,

$$r=r_{n-i-1}=2^{n-i}+2^{n-i-1}-1,$$

so

$$(\pi_n^{r+1})=(\pi_i\pi_{i+1}).$$

Now we deal with the case $i=1$. By Corollary to Theorem 2, we have already determined $f_n(2, 0, 0)$, but we will give another proof using Theorem 3 here. First, assume $n=2$. Then $k_3=k_2(\sqrt{2})$, and the ramification number of k_3/k_2 is 3, so by the conductor-ramification theorem, $f_2(2, 0, 0)=(\pi_2^4)=(4)$. Next, assume $n\geqq 3$. Put $M=k_n(\sqrt[2^{n-3}]{\pi_2})=k_n(\sqrt[2^{n-2}]{2})$, $M_1=k_{n+1}(\sqrt[2^{n-2}]{2})$, $M_2=k_n(\sqrt[2^{n-2}]{\pi_2})$, and $M_3=k_n(\sqrt[2^{n-1}]{2})$. Then M_1, M_2, and M_3 are three different extensions of M of degree 2, and $M_3\subset M_1M_2$. Since the set of upper ramification numbers of $k_n(\sqrt[2^{n-2}]{2})/k_n$ is disjoint from that of k_{n+1}/k_n, in the same way as in the proof of Theorem 3 we see that the ramification number t_1 of M_1/M is $\phi_{M/k_n}(2^n-1)$. By Theorem 3,

$$r_{n-3}=3\cdot 2^{n-3}-1<2^n-1,$$

so

$$(1)\qquad t_1=\phi_{M/k_n}(r_{n-3})+2^{n-3}(2^n-1-r_{n-3}).$$

On the other hand, the ramification number t_2 of M_2/M is

$$(2)\qquad \phi_{M_2/k_n}(r_{n-2})=\phi_{M/k_n}(r_{n-3})+2^{n-3}(r_{n-2}-r_{n-3}).$$

By Theorem 3,

$$2^n-1>r_{n-2}=3\cdot 2^{n-2}-1,$$

so by (1) and (2), $t_1>t_2$. Hence by the following Lemma 5, the ramification number of M_3/M is t_1, so by (1) we see that the last upper ramification number of M_3/k_n is 2^n-1. Thus the conductor of M_3/k_n is $(\pi_n^{2^n})=(4)$ by the conductor-ramification theorem. This settles the case $i=1$. Since $2^{2^i}=\pi_2^{2^{i+1}}$ for $i\geqq n-1$, $i\neq 1$, we have $f_n(2^i, 0, 0)=(1)$ for $i\geqq n-1$, $i\neq 1$.

ANOTHER PROOF OF COROLLARY TO THEOREM 3. If $2\leqq i\leqq n-2$, then $(\alpha, 2^{2^i})_n=(\alpha, -2^2)_n^{2^{i-1}}$. By (ii) of Corollary to Theorem 2, $f_n(2, 0, 1)=(\pi_n^{c_n})$ with $c_n=2^{n-1}+2^{n-2}$. Since $1<c_n<2^n$, by [**14**], Lemma 12 we have $f_n(2^i, 0, 0)=(\pi_i\pi_{i+1})$.

LEMMA 5. *Let l be any prime number. Let M be a finite extension of $\boldsymbol{Q}_l$ and let M_i/M be a fully ramified cyclic extension of degree l with ramification number t_i for $i=1, 2$. Assume $t_1>t_2$. Let M_3/M be any subextension of M_1M_2/M of degree l such that $M_2\neq M_3$. Then the ramification number of M_3/M is t_1.*

PROOF. Put $L=M_1M_2$. By the transitivity of the Hasse function,

$$\phi_{L/M}=\phi_{L/M_1}\circ\phi_{M_1/M}=\phi_{L/M_2}\circ\phi_{M_2/M}.$$

Hence the graph of $y=\phi_{L/M}(x)$ bends at $x=t_1$, t_2. Since $t_1\neq t_2$, the upper ramification numbers of L/M are t_2, t_1, i.e., the ramification groups of L/M are

$$\mathrm{Gal}(L/M)=G=\cdots=G^{(t_2)}\supsetneqq G^{(t_2+1)}=\cdots=G^{(t_1)}\supsetneqq G^{(t_1+1)}=\{1\}.$$

By Herbrand's theorem,

$$(G/H_2)^{(i)}=G^{(i)}H_2/H_2,$$

where $H_2=\mathrm{Gal}(L/M_2)$. Since the ramification number of M_2/M is t_2,

$$(G/H_2)^{(t_2+1)}=1,\quad\text{so}\quad G^{(t_2+1)}\subseteqq H_2.$$

Hence $H_2=G^{(t_2+1)}=G^{(t_1)}$. Put $H_3=\mathrm{Gal}(L/M_3)$. Then

$$\begin{aligned}(G/H_3)^{(t_1)}&=G^{(t_1)}H_3/H_3\\&=H_2H_3/H_3\\&\neq\{1\},\end{aligned}$$

since $H_2\neq H_3$. On the other hand,

$$(G/H_3)^{(t_1+1)}=G^{(t_1+1)}H_3/H_3=\{1\}.$$

Thus we have the assertion.

In the same way of the proof of Theorem 3, we have the following

THEOREM 4. *Let l be any odd prime number and put $k_m=\boldsymbol{Q}_l(\zeta_{l^m})$ for $m\geqq 1$. Let π be any prime element of k_1. Then $k_m(\sqrt[l^m]{\pi})/k_m$ is a fully ramified cyclic extension of degree l^m with upper ramification numbers r_i $(1\leqq i\leqq m)$:*

$$r_i=\begin{cases}2l^i-1 & \text{for } 1\leqq i\leqq m-1,\\ l^m+l^{m-1}-1 & \text{for } i=m.\end{cases}$$

As a corollary, taking $\pi=\sqrt[l-1]{-l}$, we have the following special case of Coleman-McCallum [2], Theorem 6.1. (For $i=1$, Rohrlich [15], Proposition 4.)

COROLLARY. *If l is an odd prime number and $m\geqq 1$, then*

$$f_m(l^i,0,0)=\begin{cases}(l\pi_1^2)=(\pi_1^{l+1}) & \text{for } i=0,\\ (\pi_1^2) & \text{for } 1\leqq i\leqq m-1,\\ (1) & \text{for } i\geqq m.\end{cases}$$

By Theorem 1 and Corollaries to Theorems 2 and 3, we have directly the following complete determination of $f_n(g,h,s)$:

THEOREM 5.

$$f_n(g,\ h,\ s)=\begin{cases}(8) & \text{if } \nu(g)=0 \text{ (i.e., } j=0),\\ (4) & \text{if } \nu(g)=1 \text{ and } s=0 \text{ or}\\ & \text{if } \nu(g)\geqq 2 \text{ and } s=1,\\ (\pi_j) & \text{if } 1\leqq j\leqq n-2,\ \nu(g)>\nu(h)+1, \text{ and } s=0 \text{ or}\\ & \text{if } \nu(g)\geqq\nu(h)+1=n-1,\ \nu(g)\neq 1, \text{ and } s=0 \text{ or}\\ & \text{if } 1=\nu(g)=\nu(h)+1,\ s=1, \text{ and } n=2,\\ (\pi_j\pi_{j+1}) & \text{if } 2\leqq j\leqq n-2,\ \nu(g)\leqq\nu(h)+1, \text{ and } s=0 \text{ or}\\ & \text{if } \nu(g)=1,\ s=1, \text{ and } n\geqq 3,\\ (1) & \text{if } j\geqq n \text{ and } s=0 \text{ or if } n-1=\nu(g)<\nu(h)+1,\ n\geqq 3,\\ & \text{and } s=0 \text{ or}\\ & \text{if } 1=\nu(g)<\nu(h)+1,\ s=1, \text{ and } n=2,\end{cases}$$

where $j=\min(\nu(g),\ \nu(h)+1)$ *and* ν *is the normalized additive valuation of* $\boldsymbol{Z}_2$.

§ 2. Conductor of the Jacobi sum Hecke character for a power of two.

In this section, we will show how we have to modify the arguments in [**13**], to obtain the complete determination of the conductor $C_{2^n}^{(a)}$ for the Jacobi sum Hecke character (see Corollary to Theorem 9).

We assume $n\geqq 2$, and retain all the notations in [**13**] putting $l=2$. We recall the definition of $\delta^{(n)}$:

$$\delta^{(n)}(\alpha)=\frac{-1}{2^{n-1}}\mathrm{Tr}_{K_n/K}\left(\zeta_{2^n}\alpha^{-1}\frac{d\alpha}{d\pi_n}\right)$$

$$=\frac{-1}{2^{n-1}}\mathrm{Tr}_{K_n/K}(\delta_n(\alpha))$$

for $\alpha\in U_n^{(1)}$. Here, K is any fixed finite unramified extension of $\boldsymbol{Q}_2$, $K_n=K(\zeta_{2^n})$, and $U_n^{(1)}$ is the group of principal units in K_n.

We modify [**13**], Lemma 1 as follows:

LEMMA 6. *Let the notation and assumptions be as above. Then* $\delta^{(n)}$ *is a well-defined homomorphism of* $U_n^{(1)}$ *to* $\mathcal{O}_K/2^{n-1}\mathcal{O}_K$ *satisfying the following properties* (i)$\sim$(v) *for* $\alpha\in U_n^{(1)}$:

(i) $\delta^{(n)}(\alpha^{\sigma_a})\equiv a\delta^{(n)}(\alpha) \pmod{2^{n-1}\mathcal{O}_K}$ *for* $a\in\boldsymbol{Z}_2^{\times}$.

(ii) $\delta^{(n)}(\zeta_{2^n})\equiv 1 \pmod{2^{n-1}\mathcal{O}_K}$.

(iii) $\delta^{(n)}(\alpha)\equiv -c[1+4,\ \alpha]_n \pmod{2^{n-1}\mathcal{O}_K}$ *if* $\alpha\in U_n^{(1)}\cap\boldsymbol{Q}_2(\zeta_{2^n})$, *where* $c=\left(\frac{1}{2}\log(1+4)\right)^{-1}\in 2^{-1}(1+2\boldsymbol{Z}_2)$ *and* log *is the 2-adic logarithm.*

(iv) $\delta^{(n)}(\alpha)\equiv 0 \pmod{2^{n-1}\mathcal{O}_K}$ *if* $\alpha\equiv 1 \pmod 2$ *and* $\alpha\in\boldsymbol{Q}_2(\zeta_{2^n})$.

(v) $\delta^{(n+1)}(\alpha')\equiv\delta^{(n)}(N_{n+1,n}(\alpha')) \pmod{2^{n-1}\mathcal{O}_K}$, *where* $\alpha'\in U_{n+1}^{(1)}$ *and* $N_{n+1,n}$ *is the norm of* K_{n+1} *to* K_n.

PROOF. Since the different of K_n/K is (2^{n-1}), $\mathrm{Tr}_{K_n/K}(D_n)=2^{2n-2}\mathcal{O}_K$. Hence by Iwasawa [7], Lemmas 3 and 4, (i), $\delta^{(n)}$ is a well-defined homomorphism.

(i) This follows directly from Iwasawa [7], Lemma 4, (ii).

(ii) This follows directly from the definition of $\delta^{(n)}$.

(iii) Iwasawa's formula ([7], Theorem 2) is valid even if $l=2$ by Kudo [9], so the property (iii) follows directly from this.

(iv) This follows directly from Lemma 2, (iii).

(v) This follows directly from Iwasawa [7], Lemma 5. (Note that the proof is valid for $l=2$ with slight modification.)

Because of the above modification of [13], Lemma 1, (iii) we have to modify [13], Theorem 1 as follows:

THEOREM 6. *If* $a=(a_1, \cdots, a_r)\not\equiv(0, \cdots, 0) \pmod{2^n}$,

$$\delta^{(n)}(J_{2^n}^{(a)}(\mathfrak{a})) \equiv \langle 2, \mathfrak{a}\rangle g \pmod{2^{n-1}},$$

i.e.,

$$[1+4, J_{2^n}^{(a)}(\mathfrak{a})]_n \equiv -\frac{1}{2}\log(1+4)\cdot\langle 2, \mathfrak{a}\rangle g \pmod{2^n},$$

where $g=\sum_{i=0}^{r}\nu(a_i)a_i$. *Here* $\nu(0)\cdot 0=\infty\cdot 0=0$.

PROOF. Since [13], Lemmas 2 and 3 are valid even if $l=2$, using Lemma 6 in place of [13], Lemma 1 we have the assertion in the same way as the proof of [13], Theorem 1.

We modify [13], Lemma 4 as follows:

LEMMA 7 (Iwasawa [8], p. 82, line 2). *If* $a\in\boldsymbol{Z}$, $(a, 2)=1$, *then*

$$W_n(a) \equiv \frac{1}{2}\log\langle a\rangle^a \pmod{2^n},$$

where $\langle a\rangle$ *is a unique element in* $\boldsymbol{Z}_2^\times$ *such that* $\langle a\rangle\equiv 1 \pmod 4$ *and* $a/\langle a\rangle=\pm 1$.

PROOF. In Iwasawa's calculation (line 13, p. 81 through line 2, p. 82 of [8]), by using a formula

$$\log(1+x) \equiv x-\frac{x^2}{2} \pmod{x^2}$$

for $x\in 2\boldsymbol{Z}_2$, in place of a formula

$$\log(1+x) \equiv x \pmod{x^2}$$

for $x\in l\boldsymbol{Z}_l$ and odd l, we can get the desired congruence. (If we use a formula

$$\log(1+x) \equiv x \pmod{2^{-1}x^2}$$

for $x\in 2\boldsymbol{Z}_2$, then we obtain a congruence mod 2^{n-1}.)

We modify [13], Lemma 5 as follows:

LEMMA 8. *For any integer $m\geqq 1$ and any $c\in\boldsymbol{Z}$, we have the following* (i) *and* (ii):

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

$$\sum_{j=1}^{2^m-1} j^c \equiv \begin{cases} 0 \pmod{2^{m+1}} & \text{if } c\geqq 3 \text{ is odd and } m\geqq 3, \\ -2^{m-1} \pmod{2^{m+1}} & \text{if } c=2 \text{ and } m\geqq 2 \text{ or if } c=1 \text{ and } m\geqq 2, \\ 2^{m-1} \pmod{2^{m+1}} & \text{if } c\geqq 4 \text{ is even and } m\geqq 2 \text{ or if } m=1, \\ 2^m \pmod{2^{m+1}} & \text{if } c\geqq 3 \text{ is odd and } m=2. \end{cases}$$

(ii)

$$\sum_{\substack{0<j<2^m \\ (j,2)=1}} j^c \equiv \begin{cases} 0 \pmod{2^{m+1}} & \text{if } c \text{ is odd and } m\geqq 3, \\ 2^{m-1} \pmod{2^{m+1}} & \text{if } c \text{ is even and } m\geqq 2 \text{ or if } m=1, \\ 2^m \pmod{2^{m+1}} & \text{if } c \text{ is odd and } m=2. \end{cases}$$

PROOF. (i) If $m=1$ or if $c=1$, then it is trivial, so we may assume that $m\geqq 2$ and $c\geqq 2$. First, assume that c is odd. Since

$$(2^m-j)^c \equiv -j^c+2^m c j^{c-1} \pmod{2^{m+1}},$$

by pairing j^c and $(2^m-j)^c$ for $j\in\boldsymbol{Z}$, $0\leqq j<2^{m-1}$ in the sum, we get

$$\begin{aligned} \sum_{j=0}^{2^m} j^c &\equiv 2^m c \sum_{0\leqq j<2^{m-1}} j^{c-1}+(2^{m-1})^c \pmod{2^{m+1}} \\ &\equiv \begin{cases} 2^m \pmod{2^{m+1}} & \text{if } m=2, \\ 0 \pmod{2^{m+1}} & \text{if } m\geqq 3, \end{cases} \end{aligned}$$

since

$$\sum_{0\leqq j<2^{m-1}} j^{c-1} \equiv \begin{cases} 1 \pmod 2 & \text{if } m=2, \\ 0 \pmod 2 & \text{if } m\geqq 3. \end{cases}$$

This gives the desired congruences for odd $c\geqq 3$. Next, assume that c is even. Since $2B_i\in\boldsymbol{Z}_2$ for all $i\geqq 0$ by the von Staudt-Clausen (cf. e.g., [17], Theorem 5.10), using a well-known identity (cf. e.g., [17], Proposition 4.1)

$$B_c = \frac{1}{2^m}\sum_{j=1}^{2^m}(2^m)^c B_c\left(\frac{j}{2^m}\right),$$

we have easily a congruence

$$\begin{aligned} B_c &= \frac{1}{2^m}\sum_{j=1}^{2^m}(j^c+cB_1 j^{c-1}\cdot 2^m) \pmod{2^{m-1}} \\ &\equiv \frac{1}{2^m}\sum_{j=1}^{2^m} j^c - \frac{c}{2}\sum_{j=1}^{2^m} j^{c-1} \pmod{2^{m-1}} \\ &\equiv \frac{1}{2^m}\sum_{j=1}^{2^m} j^c \pmod{2^{m-1}}, \end{aligned}$$

where $B_c(X)=\sum_{i=0}^{c}\binom{c}{i}B_iX^{c-i}$ and B_i is the i-th Bernoulli number. Hence

$$(1)\qquad \sum_{j=1}^{2^m} j^c \equiv 2^m B_c \pmod{2^{m+1}}.$$

Using (1) for $m=2$, we have

$$B_c \equiv \frac{1}{4}\sum_{j=1}^{4} j^c \pmod 2$$

$$\equiv \frac{1}{4}(1+2^c+3^c) \pmod 2.$$

Since

$$3^c=(-1+4)^c \equiv 1-4c \pmod{16},$$

we have

$$(2)\qquad B_c \equiv \begin{cases} -\dfrac{1}{2} \pmod{2\boldsymbol{Z}_2} & \text{if } c=2, \\ \dfrac{1}{2} \pmod{2\boldsymbol{Z}_2} & \text{if } c\geqq 4. \end{cases}$$

By (1) and (2), we have the desired congruences for even c.

(ii) This follows from (i) in the same way as the proof of [**13**], Lemma 5, (ii).

We modify [**13**], Lemma 6 as follows:

LEMMA 9. *For* $0\leqq m\leqq n-1$, *put*

$$A=\sum_{\substack{0<t<2^n\\(t,2)=1}}\left(\left\{\frac{t}{2^{n-m}}\right\}-2^m\left\{\frac{t}{2^n}\right\}\right)(-t)^{-1}\in \boldsymbol{Z}_2.$$

Then

$$A \equiv \begin{cases} 2^{n-1} \pmod{2^n} & \text{if } m=n-2\geqq 1, \\ 2^{n-2} \pmod{2^n} & \text{if } m=n-1\geqq 2, \\ -2^{n-2} \pmod{2^n} & \text{if } m=n-1=1, \\ 0 \pmod{2^n} & \text{otherwise.} \end{cases}$$

PROOF. In the same way as the proof of [**13**], Lemma 6, using Lemma 8 in place of [**13**], Lemma 5, we have

$$A \equiv \left(\sum_{\substack{0<t_1<2^{n-m}\\(t_1,2)=1}} t_1^{-1}\right)\left(\sum_{0\leq t_2<2^m} t_2\right)-\left(\sum_{t_1} t_1^{-2}\right)\left(\sum_{t_2} t_2^2\right)\cdot 2^{n-m} \pmod{2^n}.$$

By this and Lemma 8, we have the assertion.

By using Lemma 9 in place of [**13**], Lemma 6, in the same way as the proof of [**13**], Lemma 7, we obtain the following

LEMMA 10. *Let* $a\in\boldsymbol{Z}$ *be of the form* $a=2^m a'$ *with* a', $m\in\boldsymbol{Z}$, $(a', 2)=1$, *and* $0\leqq m\leqq n-1$. *Then*

$$W_n(a)\equiv\begin{cases}2^m W_n(a')+2a \pmod{2^n} & \text{if } m=n-2\geqq 1,\\ 2^m W_n(a')+\dfrac{a}{2} \pmod{2^n} & \text{if } m=n-1\geqq 2,\\ 2^m W_n(a')-\dfrac{a}{2} \pmod{2^n} & \text{if } m=n-1=1,\\ 2^m W_n(a') \pmod{2^n} & \text{otherwise.}\end{cases}$$

By Lemmas 7 and 10, we have the following

THEOREM 7. *For any* $a\in\boldsymbol{Z}$, *we have*

$$W_n(a)\equiv\begin{cases}\dfrac{1}{2}\log\langle a\rangle^a+2a \pmod{2^n} & \text{if } \nu(a)=n-2\geqq 1,\\ \dfrac{1}{2}\log\langle a\rangle^a+\dfrac{a}{2} \pmod{2^n} & \text{if } \nu(a)=n-1\geqq 2 \text{ or if } \nu(a)=n,\\ \dfrac{1}{2}\log\langle a\rangle^a-\dfrac{a}{2} \pmod{2^n} & \text{if } \nu(a)=n-1=1,\\ \dfrac{1}{2}\log\langle a\rangle^a \pmod{2^n} & \text{otherwise.}\end{cases}$$

Here, $\langle a\rangle$ *is a unique integer satisfying* $\langle a\rangle\equiv 1 \pmod 4$ *and* $a'/\langle a\rangle\in\{\pm 1\}$ *if* $a=a'\cdot 2^m$ *with* $m\geqq 0$, $2\nmid a'$, *and* $\langle 0\rangle=1$.

PROOF. If $\nu(a)\geqq n$, then clearly

$$W_n(a)\equiv\frac{a}{2} \pmod{2^n}$$

and

$$\log\langle a\rangle^a\equiv 0 \pmod{2^{n+2}}.$$

This gives the assertion when $\nu(a)\geqq n$. The other cases follow from Lemmas 7 and 10.

COROLLARY.

$$S_{2^n}^{(a)}\equiv\frac{1}{2}\log\Big(\prod_{i=0}^{r}\langle a_i\rangle^{a_i}\Big)+T+2^{n-1}t \pmod{2^n},$$

where

$$T=T_{n-1}=\frac{1}{2}\sum_{\substack{\nu(a_i)=n-1\\ 0\leqq i\leqq r}}a_i$$

and

$$t=t_n=\begin{cases}\#\{0\leqq i\leqq r \mid \nu(a_i)=n-2 \text{ or } n\} & \text{if } n\geqq 3,\\ \#\{0\leqq i\leqq r \mid \nu(a_i)=n-1 \text{ or } n\} & \text{if } n=2.\end{cases}$$

In the same way as the proof of [**13**], Theorem 3, using Lemma 6, Theorem 6, and Corollary to Theorem 7 in place of [**13**], Lemma 1, Theorem 1, and Corollary to Theorem 2 respectively, we obtain the following

THEOREM 8. *Assume* $a=(a_1, \cdots, a_r)\not\equiv(0, \cdots, 0) \pmod{2^n}$. *Then*

$$\begin{aligned} i_{2^n}^{(a)}(\alpha) &\equiv g[2, \alpha]_n+h[1+4, \alpha]_n \pmod{2^{n-1}}\\ &\equiv\left[\prod_{i=0}^{r} a_i^{a_i}, \alpha\right]_n+2^{-1}T[1+4, \alpha]_n \pmod{2^{n-1}}\end{aligned}$$

for $\alpha\in\boldsymbol{Q}(\zeta_{2^n})$, $\alpha\equiv 1 \pmod{\pi_n}$, *where*

$$g=\sum_{i=0}^{r}\nu(a_i)a_i, \quad a_0=-\sum_{i=1}^{r}a_i,$$

$$h=cS_{2^n}^{(a)}\left(\equiv\log\left(\prod_{i=0}^{r}\langle a_i\rangle^{a_i}\right)\Big/\log(1+4)+2^{-1}T \pmod{2^{n-2}}\right),$$

$$c=\left(\frac{1}{2}\log(1+4)\right)^{-1}\in 2^{-1}(1+2\boldsymbol{Z}_2),$$

$$S_{2^n}^{(a)}=\sum_{\substack{0<t<2^n\\(t,2)=1}}\left(\sum_{i=0}^{n}\left\{\frac{a_i t}{2^n}\right\}\right)(-t)^{-1}\in\boldsymbol{Z}_2,$$

and

$$T=T_{n-1}=\frac{1}{2}\sum_{\substack{\nu(a_i)=n-1\\0\leqq i\leqq r}}a_i.$$

Here, $\nu(0)\cdot 0=\infty\cdot 0=0$ *and* $0^0=1$.

Note that $h[1+4, \alpha]_n$ is well-defined modulo 2^{n-1} if we determine $h \bmod 2^{n-2}$, since $[1+4, \alpha]_n\equiv 0 \pmod 2$ for $\alpha\equiv 1 \pmod{\pi_n}$. (Cf. The end of the proof of Theorem 1.)

In the following, we will determine $i_{2^n}^{(a)}(\alpha) \bmod 2^n$ for $\alpha\in\boldsymbol{Q}(\zeta_{2^n})$ such that $\alpha\equiv 1 \pmod{\pi_n^3}$ in terms of Hilbert norm residue symbols (see Theorem 9 below). For the purpose we need several lemmas.

For any $b\in\boldsymbol{Z}$, put

$$\eta_n(b)=\sum_{\substack{0<t<2^n\\(t,2)=1}}\left(\left\{\frac{bt}{2^n}\right\}-b\left\{\frac{t}{2^n}\right\}\right)\sigma_t^{-1}\in\boldsymbol{Z}[G_n],$$

where $G_n=\mathrm{Gal}(\boldsymbol{Q}_2(\zeta_{2^n})/\boldsymbol{Q}_2)$. The restriction homomorphism from G_{n+1} to G_n induces a homomorphism from $\boldsymbol{Z}[G_{n+1}]$ to $\boldsymbol{Z}[G_n]$. Let $\eta'_{n+1}(b)$ denote the image of $\eta_{n+1}(b)$ by the homomorphism. For the relation between $\eta'_{n+1}(b)$ and $\eta_n(b)$, we have the following

LEMMA 11. *Let the notation be as above and write* $b=2^m\cdot b'$ *with* m, $b'\in\boldsymbol{Z}$, $m\geqq 0$, *and* $(b', 2)=1$. *Then*

$$\eta'_{n+1}(b)=\begin{cases}\eta_n(b)+\dfrac{1-b}{2}N_n & \text{if } m=0,\\ \eta_n(b)-\sigma_{-b'}\Omega_{n,m}+\left(1-\dfrac{b}{2}\right)N_n & \text{if } 1\leqq m\leqq n-1,\\ \eta_n(b)+\left(1-\dfrac{b}{2}\right)N_n & \text{if } m=n,\\ \eta_n(b)-\dfrac{b}{2}N_n & \text{if } m\geqq n+1,\end{cases}$$

where

$$N_n=\sum_{\substack{0<t<2^n\\(t,2)=1}}\sigma_t\in\boldsymbol{Z}[G_n]$$

and

$$\Omega_{n,m}=\sum_{\substack{0<t<2^n\\(t,2)=1\\0<t'<2^{n-m}}}\sigma_t^{-1}\in\boldsymbol{Z}[G_n].$$

Here t' *is a unique integer satisfying* $t'\equiv t \pmod{2^{n-m+1}}$ *and* $0<t'<2^{n-m+1}$.

PROOF. Put

$$\bar{\eta}_n(b)=\sum_{\substack{0<t<2^n\\(t,2)=1}}\left\{\frac{bt}{2^n}\right\}\sigma_{-t}^{-1}\in\boldsymbol{Q}[G_n]$$

and

$$\tilde{\eta}_n(b)=\sum_{\substack{0<t<2^n\\(t,2)=1}}b\left\{\frac{t}{2^n}\right\}\sigma_{-t}^{-1}\in\boldsymbol{Q}[G_n].$$

Then $\eta_n(b)=\bar{\eta}_n(b)-\tilde{\eta}_n(b)$. Let $\bar{\eta}'_{n+1}(b)$ and $\tilde{\eta}'_{n+1}(b)$ denote the images of $\bar{\eta}_{n+1}(b)$ and $\tilde{\eta}_{n+1}(b)$ by the restriction homomorphism from $\boldsymbol{Q}[G_{n+1}]$ to $\boldsymbol{Q}[G_n]$ respectively. Then $\eta'_{n+1}(b)=\bar{\eta}'_{n+1}(b)-\tilde{\eta}'_{n+1}(b)$, so

$$\eta'_{n+1}(b)-\eta_n(b)=(\bar{\eta}'_{n+1}(b)-\bar{\eta}_n(b))-(\tilde{\eta}'_{n+1}(b)-\tilde{\eta}_n(b)). \tag{1}$$

Since $\{bt/2^n\}$ depends only on $t \bmod 2^n$,

$$\begin{aligned}\bar{\eta}_n(b)&=\sum_{t\in(\boldsymbol{Z}/2^n\boldsymbol{Z})^\times}\left\{\frac{bt}{2^n}\right\}\sigma_{-t}^{-1}\\&=\sum_{t\in(\boldsymbol{Z}/2^n\boldsymbol{Z})^\times}\left\{\frac{b't}{2^{n-m}}\right\}\sigma_{-t}^{-1}.\end{aligned}$$

Putting $b't=t_1$ and writing t_1 as t again,

$$\bar{\eta}_n(b)=\sigma_{b'}\sum_{\substack{0<t<2^n\\(t,2)=1}}\left\{\frac{t}{2^{n-m}}\right\}\sigma_{-t}^{-1}. \tag{2}$$

Hence

$$(3)\qquad \bar{\eta}_{n+1}(b)=\sigma_{b'}\sum_{\substack{0<t<2^{n+1}\\(t,2)=1}}\left\{\frac{t}{2^{n-m+1}}\right\}\sigma_{-t}^{-1}\in \boldsymbol{Q}[G_{n+1}].$$

If we write t in (3) as $t=t''+2^nc$ with $c=0, 1$, $0<t''<2^n$, and $(t'', 2)=1$ then

$$(4)\qquad \left\{\frac{t}{2^{n-m+1}}\right\}=\begin{cases}\dfrac{t''}{2^{n+1}}+\dfrac{c}{2} & \text{if } m=0,\\[2ex] \left\{\dfrac{t''}{2^{n-m+1}}\right\} & \text{if } m\geqq 1.\end{cases}$$

First, assume $m=0$. Then by (3) and (4) we have

$$\begin{aligned}\bar{\eta}'_{n+1}(b)&=\sigma_{b'}\sum_{c,t''}\left(\frac{c}{2}+\frac{t''}{2^{n+1}}\right)\sigma_{-t''}^{-1}\\&=\frac{1}{2}\sigma_{b'}N_n+\sigma_{b'}\sum_{t''}\frac{t''}{2^n}\sigma_{-t''}^{-1},\end{aligned}$$

so by (2) we have

$$(5)\qquad \bar{\eta}'_{n+1}(b)-\bar{\eta}_n(b)=\frac{1}{2}N_n \quad \text{if } m=0.$$

Next, assume $m\geqq 1$. Then by (3) and (4),

$$\begin{aligned}\bar{\eta}'_{n+1}(b)&=\sigma_{b'}\sum_{c,t''}\left\{\frac{t''}{2^{n-m+1}}\right\}\sigma_{-t''}^{-1}\\&=2\sigma_{b'}\sum_{t''}\left\{\frac{t''}{2^{n-m+1}}\right\}\sigma_{-t''}^{-1}.\end{aligned}$$

Hence

$$(6)\qquad \bar{\eta}'_{n+1}(b)-\bar{\eta}_n(b)=\sigma_{-b'}\sum_{\substack{0<t<2^n\\(t,2)=1}}a_t(n, m)\sigma_t^{-1}$$

if $m\geqq 1$, where

$$a_t(n, m)=2\left\{\frac{t}{2^{n-m+1}}\right\}-\left\{\frac{t}{2^{n-m}}\right\}.$$

If $m\geqq n+1$, then $a_t(n, m)=0$, so we can assume $1\leqq m\leqq n$. We can write t in (6) as $t=2^{n-m+1}d+t'$ with $0<t'<2^{n-m+1}$, $(t', 2)=1$, and $0\leqq d<2^{m-1}$. If $t'<2^{n-m}$, then

$$a_t(n, m)=\frac{2t'}{2^{n-m+1}}-\frac{t'}{2^{n-m}}=0.$$

If $2^{n-m}<t'<2^{n-m+1}$, then

$$a_t(n, m)=1.$$

In fact, $a_t(n, m)=x-\{x\}$, where $x=t'/2^{n-m}$. Then $1<x<2$ and $0<\{x\}<1$, so $0<x-\{x\}<2$ and $x-\{x\}\in\boldsymbol{Z}$, hence $x-\{x\}=1$. Hence by (6),

$$\bar{\eta}'_{n+1}(b)-\bar{\eta}_n(b)=\sigma_{-b'}\sum_{\substack{0<t<2^n\\(t,2)=1\\t'>2^{n-m}}}\sigma_t^{-1}$$

$$=\sigma_{-b'}(N_n-\Omega_{n,m}),$$

so

$$(7)\qquad \bar{\eta}'_{n+1}(b)-\bar{\eta}_n(b)=\begin{cases} N_n-\sigma_{-b'}\Omega_{n,m} & \text{if } 1\leqq m\leqq n,\\ 0 & \text{if } m\geqq n+1,\end{cases}$$

where $\Omega_{n,n}=0$. In the same way as the proof of (5),

$$(8)\qquad \tilde{\eta}'_{n+1}(b)-\tilde{\eta}_n(b)=\frac{b}{2}N_n$$

for any $m\geqq 0$. By (1), (5), (7), and (8), we have the assertion.

LEMMA 12. *Assume* $1\leqq m\leqq n-1$ *and let* $\Omega_{n,m}$ *be as in Lemma* 11. *Then*

$$\Omega_{n,m}=\Big(\sum_{\substack{0<t<2^{n-m}\\(t,2)=1}}\sigma_t^{-1}\Big)N_{n,n-m+1}\quad \textit{in } G_n.$$

PROOF. By definition

$$(1)\qquad \Omega_{n,m}=\sum_{0\leqq d<2^{m-1}}\ \sum_{\substack{0<t'<2^{n-m}\\(t',2)=1}}\sigma_{2^{n-m+1}d+t'}^{-1}.$$

If we fix t', then

$$(2)\qquad \sum_{0\leqq d<2^{m-1}}\sigma_{2^{n-m+1}d+t'}^{-1}=\sigma_{t'}^{-1}\cdot N_{n,n-m+1}\quad \text{in } G_n.$$

In fact, each term of the left side is equal to $\sigma_{t'}^{-1}$ on $\boldsymbol{Q}_2(\zeta_{2^{n-m+1}})$ and different from each other on $\boldsymbol{Q}_2(\zeta_{2^n})$. By (1) and (2) we have the assertion.

LEMMA 13. *Assume* $2\leqq t\leqq n-2$, *and put* $d=2^t$, $\sigma=\sigma_{1+d}$, *and* $\pi=\pi_n$. *Let* i *be any integer such that* $i\geqq 2$. *Then the following* (i), (ii), *and* (iii) *hold.*

(i) *If* i *is even, then*

$$(1+\pi^i)^{1+\sigma}\equiv 1+\pi^{2i}\pmod{\pi^{i+d}}.$$

In particular,

$$(1+\pi^i)^{1+\sigma}\equiv 1\pmod{\pi^{i+d}}\quad \textit{for } i\geqq d.$$

(ii) *If* i *is odd, then*

$$(1+\pi^i)^{1+\sigma}\equiv 1+\pi^{2i}+\pi^{i+d-1}+\pi^{i+d}\pmod{\pi^{i+d+1}}.$$

In particular,

$$(1+\pi^i)^{1+\sigma}\equiv 1+\pi^{i+d-1}+\pi^{i+d}\pmod{\pi^{i+d+1}}\quad \textit{for } i\geqq d+1.$$

(iii) *If i is odd, then*

$$(1+\pi^i)^{1+\sigma_{-1}} \equiv 1+\pi^{i+1} \pmod{\pi^{i+2}}.$$

PROOF. Put $\zeta=\zeta_{2^n}$. Since $\pi=1-\zeta$,

$$\begin{aligned}\pi^\sigma-\pi &= \zeta(1-\zeta^d)\\ &\equiv (1-\pi)\pi^d \pmod 2.\end{aligned}$$

Hence

$$\pi^\sigma \equiv \pi(1+\pi^{d-1}+\pi^d) \pmod 2. \tag{1}$$

(i) By (1), we can write

$$\pi^{\sigma-1} = 1+\lambda\pi^{d-1}$$

with some $\lambda\in \boldsymbol{Z}_2[\zeta]$. Taking the i-th power of both sides,

$$\begin{aligned}(\pi^i)^{\sigma-1} &\equiv 1+i\lambda\pi^{d-1} \pmod{\pi^d}\\ &\equiv 1 \pmod{\pi^d},\end{aligned}$$

since i is even. Hence

$$(\pi^i)^\sigma \equiv \pi^i \pmod{\pi^{i+d}}, \tag{2}$$

so

$$\begin{aligned}(1+\pi^i)^{1+\sigma} &\equiv (1+\pi^i)^2 \pmod{\pi^{i+d}}\\ &\equiv 1+\pi^{2i} \pmod{\pi^{i+d}},\end{aligned}$$

since $t\leqq n-1$ implies $2\pi^i\equiv 0 \pmod{\pi^{i+d}}$. Hence we have the first congruence. The second one follows from the first one.

(ii) Taking the i-th power of both sides of (1),

$$(\pi^i)^\sigma \equiv \pi^i(1+i\pi^{d-1}+i\pi^d) \pmod{\pi^{i+2d-2}},$$

since $t\leqq n-2$ implies $2\pi^{i-1}\equiv 0 \pmod{\pi^{i+2d-2}}$. Hence

$$(\pi^i)^\sigma \equiv \pi^i+\pi^{i+d-1}+\pi^{i+d} \pmod{\pi^{i+2d-2}}, \tag{3}$$

since i is odd. So

$$(1+\pi^i)^{1+\sigma} \equiv (1+\pi^i)(1+\pi^i+\pi^{i+d-1}+\pi^{i+d}) \pmod{\pi^{i+2d-2}}.$$

Expanding the right side, we have the first congruence, since the inequalities $t\geqq 2$, $i\geqq 2$, and $t\leqq n-2$ imply

$$\begin{aligned}i+d+1 &\leqq i+2d-2,\\ i+d+1 &\leqq 2i+d-1,\end{aligned}$$

and $2\pi^i \equiv 0 \pmod{\pi^{i+2d-2}}$, respectively. The second one follows from the first one.

(iii) In the similar way as the proof of (1), we have

$$\pi^{\sigma_{-1}-1} \equiv 1+\pi \pmod{\pi^2},$$

so

$$(\pi^i)^{\sigma_{-1}} \equiv \pi^i+\pi^{i+1} \pmod{\pi^{i+2}}.$$

Hence

$$(1+\pi^i)^{1+\sigma_{-1}} \equiv (1+\pi^i)(1+\pi^i+\pi^{i+1}) \pmod{\pi^{i+2}}.$$

Expanding the right side and using the congruences

$$\pi^{2i} \equiv 2\pi^i \equiv 0 \pmod{\pi^{i+2}},$$

we have the assertion.

LEMMA 14. *For any integer* $m \geqq 1$, *put*

$$\Omega'_m = (1+\sigma_{-1})\prod_{i=2}^{m}(1+\sigma_{1+2i}) = (1+\sigma_{-1})(1+\sigma_5)\cdots(1+\sigma_{1+2m}).$$

Then the following (i), (ii), *and* (iii) *hold.*

(i) *If* $2 \leqq m \leqq n-2$ *and* $j \geqq a_{n,m}$, *then*

$$(1+\pi_n^j)^{\Omega'_{m-1}} \equiv \begin{cases} -1 \pmod{2\pi_n} & \text{if } m=2 \text{ and } j=a_{n,m}, \\ 1 \pmod{2\pi_n} & \text{otherwise,} \end{cases}$$

where $a_{n,m}=3+(2^{n-2}+2^{n-3}+\cdots+2^m)$.

(ii) *If* $n \geqq 4$ *and* $j \geqq 3+2^{n-2}$, *then*

$$(1+\pi_n^j)^{\Omega'_{n-3}} \equiv \begin{cases} -1 \pmod{2\pi_n} & \text{if } n=4 \text{ and } j=3+2^{n-2}, \\ 1 \pmod{2\pi_n} & \text{otherwise.} \end{cases}$$

(iii) *If* $n \geqq 3$, *then*

$$(1+\pi_n^i)^{\Omega'_{n-2}} \equiv \begin{cases} -1 \pmod{2\pi_n} & \text{if } i=3, \\ 1 \pmod{2\pi_n} & \text{if } i \geqq 4. \end{cases}$$

PROOF. For simplicity, put $\pi=\pi_n$.

(i) We will prove it by induction on m. If $m=2$, then $a_{n,2}=2^{n-1}-1$ and $\Omega'_1=1+\sigma_{-1}$. Hence the assertion follows from (iii) of Lemma 13. Now assume $m \geqq 3$ and put $d=2^{m-1}$. By (i) and (ii) of Lemma 13, we can write

$$(1+\pi^j)^{1+\sigma_{1+d}} \equiv \prod_{a=1}^{s}(1+\pi^{j_a}) \pmod{2}, \tag{1}$$

where $j_1<j_2<\cdots<j_s$, and

$$\begin{cases} j_1 \geqq j+d & \text{if } j \text{ is even,} \\ j_1 = j+d-1 \text{ and } j_2 = j_1+1 & \text{if } j \text{ is odd.} \end{cases}$$

Put $A_a=(1+\pi^{j_a})^{\Omega'_{m-2}}$. If $a\geqq 3$, then

$$j_a > j+d \geqq a_{n,m-1},$$

so by the induction assumption,

$$A_a \equiv 1 \pmod{2\pi} \quad \text{for } a \geqq 3.$$

Hence by making Ω'_{m-2} operator on both sides of (1), we have

$$(2) \qquad (1+\pi^j)^{\Omega'_{m-1}} \equiv A_1 A_2 \pmod{2\pi},$$

since $x\equiv 1 \pmod 2$ implies $x^{\Omega'_{m-2}}\equiv 1 \pmod{2\pi}$. If j is even, then $j>a_{n,m}$, so

$$j_1 \geqq j+d > a_{n,m}+d = a_{n,m-1},$$

i.e., $j_1>a_{n,m-1}$, hence by the induction hypothesis,

$$A_a \equiv 1 \pmod{2\pi} \quad \text{for } a = 1, 2,$$

so by (2) we have the assertion. Now assume that j is odd. Then we can write $j_1=2j'_1$ with $j'_1\in \boldsymbol{Z}$. Since

$$j'_1 = (j-1)/2+2^{m-2} \geqq 1+(2^{n-3}+\cdots+2^{m-1})+2^{m-2} \geqq a_{n-1,m-1},$$

we have

$$j'_1 \geqq a_{n-1,m-1},$$

where the equality holds if and only if $j=a_{n,m}$ and $m=3$. Since $\pi^2\equiv\pi_{n-1}$ (mod 2), we have

$$A_1 \equiv (1+\pi_{n-1}^{j'_1})^{\Omega'_{m-2}} \pmod{2\pi}.$$

Since $j_2=j+d\geqq a_{n,m-1}$ and since the equality holds if and only if $j=a_{n,m}$, by the induction hypothesis we have

$$A_1 \equiv A_2 \equiv \begin{cases} -1 \pmod{2\pi} & \text{if } m=3 \text{ and } j=a_{n,m}, \\ 1 \pmod{2\pi} & \text{otherwise,} \end{cases}$$

so $A_1A_2\equiv 1 \pmod{2\pi}$. Hence by (2) we have the assertion.

(ii) This is a special case $m=n-2$ of (i).

(iii) We will prove it by induction on n. If $n=3$, then the assertion follows from (iii) of Lemma 13, so we may assume $n\geqq 4$. First, assume that i is even. By (i) of Lemma 13, we can write

$$(3) \qquad (1+\pi^i)^{1+\sigma_{1+2^{n-2}}} \equiv (1+\pi_{n-1}^i)\prod_{a=1}^{s}(1+\pi^{j_a}) \pmod 2,$$

where $i+2^{n-2} \leqq j_1 < j_2 < \cdots < j_s$. Since $i \geqq 4$, by (ii) we have

$$(1+\pi^{j_a})^{\Omega'_{n-3}} \equiv 1 \pmod{2\pi}$$

for $a \geqq 1$. On the other hand, by the induction hypothesis,

$$(1+\pi_{n-1}^{i})^{\Omega'_{n-3}} \equiv 1 \pmod{2\pi}.$$

Hence by making Ω'_{n-3} operate on both side of (3),

$$(1+\pi^{i})^{\Omega'_{n-2}} \equiv 1 \pmod{2\pi}.$$

(Alternatively, $\pi^i \equiv \pi_{n-1}^{i'} \pmod 2$ with $i=2i'$, so

$$(1+\pi^{i})^{\Omega'_{n-2}} \equiv (1+\pi_{n-1}^{i'})^{\Omega'_{n-2}} \pmod{2\pi}.$$

Since the right side is equal to $N_{n-1}(1+\pi_{n-1}^{i'})$, it is 1 (mod 4) as is well-known.) Now assume that i is odd. By (ii) of Lemma 13, we can write

$$(4) \qquad (1+\pi^{i})^{1+\sigma_{1+2^{n-2}}} \equiv (1+\pi_{n-1}^{i})(1+\pi_{n-1}^{i'}) \prod_{a=1}^{s} (1+\pi^{j_a}) \pmod 2,$$

where $i'=(i-1)/2+2^{n-3}$ and $i+2^{n-2}=j_1<j_2<\cdots<j_s$. By (ii) we have

$$(5) \qquad (1+\pi^{j_a})^{\Omega'_{n-3}} \equiv \begin{cases} -1 \pmod{2\pi} & \text{if } a=1,\ i=3, \text{ and } n=4, \\ 1 \pmod{2\pi} & \text{otherwise.} \end{cases}$$

By making Ω'_{n-3} operate on both sides of (4), we have

$$(6) \qquad (1+\pi^{i})^{\Omega'_{n-2}} \equiv (1+\pi_{n-1}^{i})^{\Omega'_{n-3}}(1+\pi_{n-1}^{i'})^{\Omega'_{n-3}}(1+\pi^{j_1})^{\Omega'_{n-3}} \pmod{2\pi}.$$

If $i=3$ and $n=4$, then $i'=3$, so by the proof in the case $n=3$, each term of the right side of (6) is $-1 \pmod{2\pi}$, so we have the assertion in this case. Otherwise, $i' \geqq 4$, so by the induction hypothesis,

$$(7) \qquad (1+\pi_{n-1}^{i'})^{\Omega'_{n-3}} \equiv 1 \pmod{2\pi}.$$

By (5), (6), and (7),

$$(1+\pi^{i})^{\Omega'_{n-2}} \equiv (1+\pi_{n-1}^{i})^{\Omega'_{n-3}} \pmod{2\pi}.$$

Hence by the induction hypothesis we have the assertion.

LEMMA 15. *Assume $n \geqq 3$ and put*

$$\Omega_{n-2} = \sum_{\substack{0<t<2^{n-1} \\ (t,2)=1}} \sigma_t^{-1} \in \boldsymbol{Z}[G_n].$$

Let $x \in \boldsymbol{Q}_2(\zeta_{2^n})$ be such that $x \equiv 1 \pmod{\pi_n^2}$. Then

$$x^{\Omega_{n-2}} \equiv x^{\Omega'_{n-2}} \pmod{2\pi_n},$$

where Ω'_{n-2} is as in Lemma 14.

PROOF. Put

$$U_n^{(m)} = \{x \in \boldsymbol{Q}_2(\zeta_{2^n}) \mid x \equiv 1 \pmod{\pi_n^m}\}$$

for $m \geqq 1$. In the same way as the proof of (2) and (3) in the proof of Lemma 13, we have

$$(\pi^i)^\sigma \equiv \pi^i \pmod{2\pi_n}$$

if $\sigma = \sigma_{1+2^{n-1}}$ and $i \geqq 2$. Hence

$$x^\sigma \equiv x \pmod{2\pi_n},$$

since $x = 1 + \sum_{i=2}^{\infty} \lambda_i \pi_n^i$ with $\lambda_i \in \boldsymbol{Z}$. This implies that the Galois group $G(\boldsymbol{Q}_2(\zeta_{2^n})/\boldsymbol{Q}_2(\zeta_{2^{n-1}}))$ acts trivially on the group

$$M = U_n^{(2)}/U_n^{(1+2^{n-1})}.$$

Thus M becomes G_{n-1}-module naturally. Hence

$$\begin{aligned} \tilde{x}^{\Omega_{n-2}} &= N_{n-1}(\tilde{x}) \\ &= \tilde{x}^{\Omega'_{n-2}}, \end{aligned}$$

where $\tilde{x} = x \bmod U_n^{(1+2^{n-1})}$. This gives the assertion.

By Lemmas 11, 12, 14, and 15, we will calculate $x^{\omega_{n+1}(a)-\omega_n(a)} \bmod 2\pi_n$ for $x \in \boldsymbol{Q}_2(\zeta_{2^n})$ such that $x \equiv 1 \pmod{\pi_n^3}$.

LEMMA 16. *Let $x \in \boldsymbol{Q}_2(\zeta_{2^n})$ be such that $x \equiv (1+\pi_n^3)^j \pmod{\pi_n^4}$ with $j \in \boldsymbol{Z}$. Then the following* (i) *and* (ii) *hold.*

(i)

$$x^{\eta_{n+1}(b)-\eta_n(b)} \equiv \begin{cases} (-1)^j \pmod{2\pi_n} & \text{if } 1 \leqq m \leqq n-2, \\ 1 \pmod{2\pi_n} & \text{otherwise,} \end{cases}$$

where $\eta_n(b)$ is as in Lemma 11 *and $m = \nu(b)$.*

(ii) *If $a = (a_1, \cdots, a_r) \in \boldsymbol{Z}^r$, then*

$$x^{\omega_{n+1}(a)-\omega_n(a)} \equiv (-1)^{jr'} \pmod{2\pi_n}.$$

Here $r' = r'_n = \#\{0 \leqq i \leqq r \mid 1 \leqq \nu(a_i) \leqq n-2\}$, and $a_0 = -\sum_{i=1}^r a_i$.

PROOF. (i) Since $N_n(x) \equiv 1 \pmod 4$ as is well-known, by Lemma 11 we have directly the assertion unless $1 \leqq m \leqq n-1$. If $m = n-1$, then $\Omega_{n,m} = N_{n,2}$, so

$$x^{\Omega_{n,m}} \equiv 1 \pmod{\pi_2^3}$$

by Hasse [**4**] (see also Serre [**16**], Chap. V, § 3), hence we have assertion in this case by Lemma 11. So we may assume $1 \leqq m \leqq n-2$. By Lemma 12,

(1) $$x^{\Omega_{n,m}} = x'^{\Omega_{n-m-1}},$$

where $x'=N_{n,n-m+1}(x)$ and $\Omega_{n-m-1}=\sum_{\substack{0<t<2^{n-m}\\(t,2)=1}}\sigma_t^{-1}$. Since $n-m+1\geqq 3$, by Hasse [4] we have

$$x' \equiv (1+\pi_{n-m+1}^3)^j \pmod{\pi_{n-m+1}^4}.$$

So by Lemma 15,

(2) $$x'^{\Omega_{n-m-1}} \equiv x'^{\Omega'_{n-m-1}} \pmod{2\pi_{n-m+1}}.$$

By (1) and (2),

$$x^{\Omega_{n,m}} \equiv x'^{\Omega'_{n-m-1}} \pmod{2\pi_n}.$$

Hence by Lemma 11 and (iii) of Lemma 14 we have the assertion.

(ii) By definition,

$$\omega_n(a) = \sum_{i=0}^{r} \eta_n(a_i) - N_n,$$

so we have directly the assertion by (i).

By Lemma 16 and Theorem 12 in § 3, we will prove the following Lemma 17, which is a key to the proof of Theorem 9.

LEMMA 17. *Let $\beta\in\boldsymbol{Q}(\zeta_{2^{n+1}})$ be such that $\beta\equiv(1+\pi_{n+1}^3)^j \pmod{\pi_{n+1}^4}$ with $j\in\boldsymbol{Z}$. Assume that $a=(a_1,\cdots,a_r)\in\boldsymbol{Z}^r$ and $a\not\equiv(0,\cdots,0) \pmod{2^n}$. Then*

$$i_{2^n}^{(a)}(N_{n+1,n}(\beta)) \equiv i_{2^{n+1}}^{(a)}(\beta)+jr'\cdot 2^{n-1} \pmod{2^n},$$

where $r'=r'_n$ is as in Lemma 16.

PROOF. Recall that

(1) $$J_{2^n}^{(a)}((x)) = \zeta_{2^n}^{i(x)} x^{\omega_n(a)} \text{ with } i(x) = i_{2^n}^{(a)}(x) \in \boldsymbol{Z}/2^n\boldsymbol{Z},$$

for any $x\in\boldsymbol{Q}(\zeta_{2^n})$ such that $x\equiv 1 \pmod{\pi_n}$. By taking $N_{n+1,n}$ of both sides of (1) (replacing n by $n+1$ and putting $x=\beta$), we have

(2) $$J_{2^{n+1}}^{(a)}((\alpha')) = (-\zeta_{2^n})^{i'(\beta)}\alpha'^{\omega_{n+1}(a)},$$

where $\alpha'=N_{n+1,n}(\beta)$ and $i'(\beta)=i_{2^{n+1}}^{(a)}(\beta)$. On the other hand, putting $x=\alpha'$ in (1),

(3) $$J_{2^n}^{(a)}((\alpha')) = \zeta_{2^n}^{i(\alpha')}\alpha'^{\omega_n(a)}.$$

By Theorem 12 in § 3,

(4) $$J_{2^{n+1}}^{(a)}((\alpha')) \equiv J_{2^n}^{(a)}((\alpha')) \pmod{2\pi_n}.$$

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

$$(-\zeta_{2^n})^{i'(\beta)}\alpha'^{\omega_{n+1}(a)} \equiv \zeta_{2^n}^{i(\alpha')}\alpha'^{\omega_n(a)} \pmod{2\pi_n},$$

i.e.,

$$(5)\qquad \zeta_{2^n}^{i(\alpha')-(1+2^{n-1})i'(\beta)} \equiv \alpha'^{\omega_{n+1}(a)-\omega_n(a)} \pmod{2\pi_n}.$$

By Hasse [4],

$$\alpha' \equiv \begin{cases} (1+\pi_n^3)^j \pmod{\pi_n^4} & \text{if } n \geqq 3, \\ 1 \pmod{\pi_n^4} & \text{if } n = 2. \end{cases}$$

By Lemma 16,

$$(6)\qquad \alpha'^{\omega_{n+1}(a)-\omega_n(a)} \equiv (-1)^{jr'} \pmod{2\pi_n}.$$

(Note that $r'=0$ if $n=2$.) By (5) and (6),

$$\zeta_{2^n}^{i(\alpha')-(1+2^{n-1})i'(\beta)} \equiv \zeta_{2^n}^{2^{n-1}jr'} \pmod{2\pi_n},$$

so $i(\alpha')-(1+2^{n-1})i'(\beta)\equiv 2^{n-1}jr' \pmod{2^n}$. Since $[1+4, \beta]_{n+1}\equiv 0 \pmod 4$ by Theorem 1, we have $i'(\beta)\equiv 0 \pmod 2$ by Theorem 8. Hence we obtain the assertion.

By Theorem 8, Lemma 17, and Theorem 15 in § 3, we will give a formula on $i_{2^n}^{(a)}(\alpha) \bmod 2^n$ for $\alpha\in\boldsymbol{Q}(\zeta_{2^n})$ such that $\alpha\equiv 1 \pmod{\pi_n^3}$ in terms of Hilbert norm residue symbols:

THEOREM 9. *Assume* $a=(a_1, \cdots, a_r)\not\equiv(0, \cdots, 0) \pmod{2^n}$. *Then*

$$\begin{aligned} i_{2^n}^{(a)}(\alpha) &= g[2, \alpha]_n + h'[1+4, \alpha]_n + s[-1, \alpha]_n \pmod{2^n} \\ &\equiv \left[\prod_{i=0}^{r} a_i^{a_i}, \alpha\right]_n + 2^{n-3}r'[1+4, \alpha]_n \pmod{2^n} \end{aligned}$$

for $\alpha\in\boldsymbol{Q}(\zeta_{2^n})$, $\alpha\equiv 1 \pmod{\pi_n^3}$, *where*

$$g = \sum_{i=0}^{r} \nu(a_i)a_i, \quad a_0 = -\sum_{i=1}^{r} a_i,$$

$$\begin{aligned} h' &= cS_{2^{n+1}}^{(a)} + 2^{n-3}r' \\ &\equiv \log\Big(\prod_{i=0}^{r} \langle a_i\rangle^{a_i}\Big) \Big/ \log(1+4) + 2^{n-3}r' \pmod{2^{n-2}}, \end{aligned}$$

$$\begin{aligned} s &= \#\{0 \leqq i \leqq r \mid a_i \equiv 1 \pmod 4\} \pmod 2 \\ &\equiv r'' + g/2 \pmod 2, \end{aligned}$$

$$c = (2^{-1}\log(1+4))^{-1} \in 2^{-1}(1+2\boldsymbol{Z}_2),$$

$r' = r'_n = 0$ *or* 1 *according as the number of* i $(0\leqq i\leqq r)$ *such that* $1\leqq\nu(a_i)\leqq n-2$ *is even or odd, and*

$$r'' = \#\{0 \leqq i \leqq r \mid (a_i, 2) = 1\}/2.$$

Here, $\nu(0)\cdot 0=\infty\cdot 0=0$ *and* $0^0=1$.

PROOF. By Theorem 8 (or Weil [18]), $i_{2^n}^{(a)}(x)\equiv 0 \pmod{2^n}$ if $x\equiv 1 \pmod{\pi_n^m}$ for a sufficiently large m, so we can extend the domain where $i_{2^n}^{(a)}$ is defined, to

$$U_n^{(1)} = \{x \in \boldsymbol{Q}_2(\zeta_{2^n}) \mid x \equiv 1 \pmod{\pi_n}\},$$

by continuity. Thus $i_{2^n}^{(a)}$ is a homomorphism from $U_n^{(1)}$ to $\boldsymbol{Z}/2^n\boldsymbol{Z}$. Put $\eta=1+\pi_2^3$. Then, as is well known, we can write

$$\alpha = \eta^m \alpha' \tag{1}$$

with $m\in\boldsymbol{Z}_2$, $\alpha'\in U_n^{(1)}$ such that $\alpha'\equiv 1 \pmod{\pi_n^3}$ and $N_n(\alpha')=1$. We can write $\alpha'=N_{n+1,n}(\beta)$ with some $\beta\in\boldsymbol{Q}_2(\zeta_{2^{n+1}})$, $\beta\equiv 1 \pmod{\pi_{n+1}^3}$. Then by Lemma 17 and Theorem 8,

$$\begin{aligned} i_{2^n}^{(a)}(\alpha') &\equiv i_{2^{n+1}}^{(a)}(\beta)+jr'\cdot 2^{n-1} \pmod{2^n} \\ &\equiv g[2,\ \beta]_{n+1}+h[1+4,\ \beta]_{n+1}+jr'\cdot 2^{n-1} \pmod{2^n}, \end{aligned}$$

so

$$i_{2^n}^{(a)}(\alpha') \equiv g[2,\ \alpha']_n+h[1+4,\ \alpha']_n+jr'\cdot 2^{n-1} \pmod{2^n}, \tag{2}$$

where $h=cS_{2^{n+1}}^{(a)}$ and $\beta\equiv(1+\pi_{n+1}^3)^j \pmod{\pi_{n+1}^4}$ with $j\in\boldsymbol{Z}$. Next, we will show

$$jr'\cdot 2^{n-1} \equiv 2^{n-3}r'[1+4,\ \alpha']_n \pmod{2^n}. \tag{3}$$

If $n=2$, then $r'=0$, so we may assume $n\geqq 3$. Then by Hasse [4],

$$\alpha' \equiv (1+\pi_n^3)^j \pmod{\pi_n^4}.$$

By Theorem 1,

$$\begin{aligned} 2^{n-3}[1+4,\ 1+\pi_n^3]_n &\equiv [(1+4)^{2^{n-3}},\ 1+\pi_n^3]_n \\ &\equiv 2^{n-1} \pmod{2^n}, \end{aligned}$$

and

$$2^{n-3}[1+4,\ x]_n \equiv 0 \pmod{2^n} \tag{4}$$

for $x\in\boldsymbol{Q}_2(\zeta_{2^n})$, $x\equiv 1 \pmod{\pi_n^4}$. This gives (3). By Artin-Hasse [1],

$$\begin{aligned} [-1,\ \alpha']_n &\equiv [\zeta_{2^n}^{2^{n-1}},\ \alpha']_n \\ &\equiv 2^{n-1}[\zeta_{2^n},\ \alpha']_n \\ &\equiv 2^{n-1}(1+2^{n-1})2^{-n}T_n(\log\alpha') \pmod{2^n}, \end{aligned}$$

so

$$[-1,\ \alpha']_n \equiv 0 \pmod{2^n}, \tag{5}$$

since $T_n(\log\alpha')=\log N_n(\alpha')=0$. Hence by (2), (3), and (5), the first desired formula holds for $\alpha=\alpha'$. Thus it suffices to prove the formula when $\alpha=\eta$, because of (1). Since

$$\begin{aligned}(2^2, \eta)_n &= (2, \eta)'_n \\ &= (2, N_{n,n-1}(\eta))_{n-1} \\ &= (2, \eta^2)_{n-1} \\ &= (2^2, \eta)_{n-1}\end{aligned}$$

for $n \geqq 3$, we have

$$(2^2, \eta)_n = (2^2, \eta)_2,$$

where $(\ ,\ )'_n$ is the Hilbert norm residue symbol in $\boldsymbol{Q}_2(\zeta_{2^n})$ for the power 2^{n-1}. In the same way,

$$(2^2, \eta)_2 = (2, N_2(\eta))_1 = -1,$$

since $N_2(\eta) \equiv 1+4 \pmod 8$. Hence

$$[2^2, \eta]_n \equiv 2^{n-1} \pmod{2^n}. \tag{6}$$

By Theorem 1,

$$[1+4, \eta]_n \equiv 0 \pmod{2^n}. \tag{7}$$

In the same way as the proof of (ii) of Theorem 2,

$$[-1, \eta]_n \equiv 2^{n-1} \pmod{2^n}. \tag{8}$$

By (6), (7), and (8), the right side of the desired first formula for $\alpha = \eta$ is equal to $(s+g/2)\cdot 2^{n-1}$, i.e., $r''\cdot 2^{n-1} \pmod{2^n}$. In fact, since $a_i \nu(a_i) \equiv 0 \pmod 4$ for $\nu(a_i) \neq 1$, we have

$$g \equiv \sum_{\substack{\nu(a_i)=1 \\ 0 \leq i \leq r}} a_i \pmod 4. \tag{9}$$

Since $\sum_{i=0}^{r} a_i = 0$, we have

$$\sum_{\substack{\nu(a_i)=0, 1 \\ 0 \leq i \leq r}} a_i \equiv 0 \pmod 4. \tag{10}$$

Since

$$\begin{aligned}\sum_{\substack{\nu(a_i)=0 \\ 0 \leq i \leq r}} a_i &\equiv s-(2r''-s) \pmod 4 \\ &\equiv 2(s-r'') \pmod 4,\end{aligned}$$

by (9) and (10) we have

$$s+g/2 \equiv r'' \pmod 2.$$

On the other hand, by Theorem 15 in § 3,

$$i_{2^n}^{(a)}(\eta) \equiv r''\cdot 2^{n-1} \pmod{2^n}.$$

Thus we have the first formula in Theorem 9. Since by Theorem 1 we have $[1+4, \alpha]_n \equiv 0 \pmod{2^2}$ for $\alpha \in \boldsymbol{Q}_2(\zeta_{2^n})$ such that $\alpha \equiv 1 \pmod{\pi_n^3}$, $h'[1+4, \alpha]_n$ is well-defined mod 2^n if we determine $h' \bmod 2^{n-2}$. By the first formula and

Corollary to Theorem 7,

$$\begin{aligned} i_{2^n}^{(a)}(\alpha) &\equiv g[2,\ \alpha]_n+\Big(\log\Big(\prod_{i=0}^{r}\langle a_i\rangle^{a_i}\Big)\Big/\log(1+4)+2^{n-3}r'\Big)[1+4,\ \alpha]_n \\ &\quad +s[-1,\ \alpha]_n \pmod{2^n} \\ &\equiv \Big[\prod_{i=0}^{r}(2^{\nu(a_i)}\langle a_i\rangle)^{a_i},\ \alpha\Big]_n+2^{n-3}r'[1+4,\ \alpha]_n \\ &\quad +s[-1,\ \alpha]_n \pmod{2^n} \\ &\equiv \Big[(-1)^{2^{r''}-s}\prod_{i=0}^{r}a_i^{a_i},\ \alpha\Big]_n+2^{n-3}r'[1+4,\ \alpha]_n \\ &\quad +s[-1,\ \alpha]_n \pmod{2^n} \\ &\equiv \Big[\prod_{i=0}^{r}a_i^{a_i},\ \alpha\Big]_n+2^{n-3}r'[1+4,\ \alpha]_n \pmod{2^n}. \end{aligned}$$

Hence we have the second formula.

REMARK.

(1) We can omit the term $2^{n-3}r'[1+4,\ \alpha]_n$ in the formula of Theorem 9 when $\alpha\equiv 1 \pmod{\pi_n^4}$, since $r'=0$ when $n=2$ and since (4) in the proof of Theorem 9 holds when $n\geqq 3$.

(2) *The formula in Theorem* 9 *holds for any* $\alpha\in\boldsymbol{Q}(\zeta_{2^n})$ *such that* $\alpha\equiv 1 \pmod{\pi_n}$ *if and only if* $I_n\equiv 0 \pmod{2^n}$, *where* I_n *is as in the corollary below.* In fact, since $\zeta_{2^n}\equiv 1+\pi_n \pmod{\pi_n^2}$ and $\zeta_{2^n}^2\equiv 1+\pi_n^2 \pmod{\pi_n^3}$, it suffices to get the condition for the formula to hold for $\alpha=\zeta_{2^n}$. By Artin-Hasse [**1**], we have

$$[2,\ \zeta_{2^n}]_n \equiv 0 \pmod{2^n},$$

$$[-1,\ \zeta_{2^n}]_n \equiv 0 \pmod{2^n},$$

and

$$[1+4,\ \zeta_{2^n}]_n \equiv -c^{-1} \pmod{2^n}.$$

(For the first one, see Rohrlich [**15**], line 3, page 105.) Hence the right side of the formula is equal to $-h'c^{-1}$, so $-S_{2^n}^{(a)}-I_n \pmod{2^n}$ by (1) in the proof of the corollary below. On the other hand, by definition we have easily

$$i_{2^n}^{(a)}(\zeta_{2^n}) \equiv -S_{2^n}^{(a)} \pmod{2^n}.$$

This gives the assertion.

(3) Theorem 9 with the above remark (2) generalizes Coleman [**3**], Theorem (6.4) (with G. Anderson). They deal with the $(a_0\cdots a_r,\ 2)=1$ and $N_n(\alpha)\equiv 1 \pmod{2^{n+2}}$ in a different method.

COROLLARY.

$$C_{2^n}^{(a)} = \begin{cases} (4) & \text{if } \nu(g)=1 \text{ and } s=0 \text{ or if } \nu(g)\geqq 2 \text{ and } s=1, \\ (\pi_{j'}) & \text{if } 1\leqq j\leqq n-2,\ \nu(g)>\nu(h')+1, \text{ and } s=0, \\ & \text{or if } \nu(g)\geqq\nu(h')+1=n-1,\ \nu(g)\neq 1,\ s=0, \text{ and } \nu(I_n)\geqq n, \\ & \text{or if } j\geqq n,\ s=0, \text{ and } \nu(I_n)=n-1, \\ & \text{or if } n-1=\nu(g)<\nu(h')+1,\ s=0,\ n\geqq 3, \text{ and } \nu(I_n)=n-1, \\ & \text{or if } 1=\nu(g)=\nu(h')+1,\ s=1,\ n=2, \text{ and } \nu(I_n)\geqq n, \\ & \text{or if } 1=\nu(g)<\nu(h')+1,\ s=1,\ n=2, \text{ and } \nu(I_n)=n-1, \\ (\pi_{j'}\pi_{j'+1}) & \text{if } 2\leqq j\leqq n-2,\ \nu(g)\leqq\nu(h')+1, \text{ and } s=0, \\ & \text{or if } \nu(g)=1,\ s=1, \text{ and } n\geqq 3, \\ & \text{or if } \nu(g)\geqq\nu(h')+1=n-1,\ \nu(g)\neq 1,\ s=0, \text{ and } \nu(I_n)=n-2, \\ & \text{or if } j\geqq n,\ s=0, \text{ and } \nu(I_n)=n-2, \\ & \text{or if } n-1=\nu(g)<\nu(h')+1,\ s=0,\ n\geqq 3, \text{ and } \nu(I_n)=n-2, \\ & \text{or if } \nu(g)=1,\ s=1,\ n=2, \text{ and } \nu(I_n)=n-2, \\ (1) & \text{if } \nu(g)\geqq\nu(h')+1=n-1,\ \nu(g)\neq 1,\ s=0, \text{ and } \nu(I_n)=n-1, \\ & \text{or if } j\geqq n,\ s=0, \text{ and } \nu(I_n)\geqq n, \\ & \text{or if } n-1=\nu(g)<\nu(h')+1,\ s=0,\ n\geqq 3, \text{ and } \nu(I_n)\geqq n, \\ & \text{or if } 1=\nu(g)=\nu(h')+1,\ s=1,\ n=2, \text{ and } \nu(I_n)=n-1, \\ & \text{or if } 1=\nu(g)<\nu(h')+1,\ s=1,\ n=2, \text{ and } \nu(I_n)\geqq n, \end{cases}$$

where

$$I_n = -T_{n-1}-2^{n-2}r'_n+2^{n-1}t'_n,$$

$$t'_n = \begin{cases} \#\{0\leqq i\leqq r \mid \nu(a_i)=n-2\} & \text{if } n\geqq 3, \\ \#\{0\leqq i\leqq r \mid \nu(a_i)=n-1\} & \text{if } n=2, \end{cases}$$

$$j=\min(\nu(g),\ \nu(h')+1),\quad j'=\min(j,\ n-1),$$

T_{n-1} is as in Corollary to Theorem 7, and g, h', s, and r'_n are as in Theorem 9.

PROOF. Since $c^{-1}\equiv -2 \pmod 8$, we have

$$\begin{aligned} c^{-1}h' &= S_{2^{n+1}}^{(a)}+2^{n-3}c^{-1}r' \\ &\equiv S_{2^{n+1}}^{(a)}-2^{n-2}r' \pmod{2^n}. \end{aligned}$$

Hence by Corollary to Theorem 7,

$$(1) \qquad c^{-1}h' \equiv S_{2^n}^{(a)}+I_n \pmod{2^n}.$$

Put $m=\nu(S_{2^n}^{(a)})$ and $m'=\nu(I_n)$ for simplicity. By definition, $m'\geqq n-2$. Put $f_n(g,\ h',\ s)=(\pi_n^d)$. If $d\geqq 4$, then $C_{2^n}^{(a)}=f_n(g,\ h',\ s)$ by Theorem 9. So we may assume $d\leqq 3$. Then $\nu(h')\geqq n-2$ by Theorem 5. If $\nu(h')=n-2$, then $m\geqq n$, $m=n-1$, or $m=n-2$ according as $m'=n-1$, $m'\geqq n$, or $m'=n-2$. If $\nu(h')\geqq n-1$,

then we have the same conditions according as $m' \geqq n$, $m'=n-1$, or $m'=n-2$. Hence by Theorems 5 and 9, $C_{2^n}^{(a)}=(1)$, (π_n^2) $(=(\pi_{n-1}))$, or (π_n^3) $(=(\pi_{n-1}\pi_n))$ according as $m \geqq n$, $m=n-1$, or $m=n-2$, if $\nu(g) \geqq \nu(h')+1=n-1$, $\nu(g) \neq 1$, and $s=0$, or if $j \geqq n$ and $s=0$, or if $n-1=\nu(g)<\nu(h')+1$, $s=0$, and $n \geqq 3$, or if $\nu(g)=1$, $s=1$, and $n=2$, since

$$i_{2^n}^{(a)}(\zeta_{2^n}) \equiv -S_{2^n}^{(a)} \pmod{2^n}.$$

Hence we have the assertion.

§ 3. Certain congruences for Gauss sums and Jacobi sums.

The purpose of this section is to prove certain congruences for Jacobi sums (see Theorems 12, 13, and 14). We used Theorem 12 for the proof of Lemma 17 in § 2, and we will use Theorem 14 to determine $i_{2^n}^{(a)}((\eta)) \bmod 2^n$ for $\eta \in \boldsymbol{Q}_2(\zeta_4)$, $\eta \equiv 1+\pi_2^3 \pmod{\pi_2^4}$ (see Theorem 15), which we used for the proof of Theorem 9 in § 2.

In this section, let l be any prime number and assume $n \geqq 2$ if $l=2$. Put $q=l$ or 4, and $f=f_n=1$ or $1+2^{n-1}$ according as l is odd or 2.

THEOREM 10. *Let $\mathfrak{p}_{n+1}$ be any prime ideal of $\boldsymbol{Q}(\zeta_{l^{n+1}})$ which is prime to l, let $\mathfrak{p}_n$ be the prime ideal of $\boldsymbol{Q}(\zeta_{l^n})$ lying below $\mathfrak{p}_{n+1}$, and let p be the prime number contained in $\mathfrak{p}_n$. Let M be the decomposition field of $\mathfrak{p}_{n+1}$ with respect to $\boldsymbol{Q}(\zeta_{l^{n+1}})/\boldsymbol{Q}(\zeta_q)$. Assume $M \subset \boldsymbol{Q}(\zeta_{l^n})$ (i.e., $\mathfrak{p}_n$ does not decompose in $\boldsymbol{Q}(\zeta_{l^{n+1}})/\boldsymbol{Q}(\zeta_{l^n})$), and put $l^d=[\boldsymbol{Q}(\zeta_{l^n}) : M]$. Then for any $a \in \boldsymbol{Z}$, we have*

$$g_{l^{n+1}}(\mathfrak{p}_{n+1}, a) \equiv \left(\frac{l}{\mathfrak{p}_n}\right)_{l^n}^{-af} g_{l^n}(\mathfrak{p}_n, af) \pmod{l^{d+1}\boldsymbol{Z}[\zeta_{pl^{n-d}}]}.$$

For simplicity, put $\chi'=\chi_{\mathfrak{p}_{n+1}}^a$, $\chi=\chi_{\mathfrak{p}_n}^a$, $k'=\boldsymbol{Z}[\zeta_{l^{n+1}}]/\mathfrak{p}_{n+1}$, $k=\boldsymbol{Z}[\zeta_{l^n}]/\mathfrak{p}_n$, $k_0=\boldsymbol{Z}[\zeta_{l^{n-d}}]/\mathfrak{p}_n \cap M$, $\psi'(x')=\zeta_p^{T'(x')}$ for $x' \in k'$, and $\psi(x)=\zeta_p^{T(x)}$ for $x \in k$, where $T'=\mathrm{Tr}_{k'/\boldsymbol{F}_p}$ and $T=\mathrm{Tr}_{k/\boldsymbol{F}_p}$ are the traces from k' and k to $\boldsymbol{F}_p$ respectively.

For our proof of Theorem 10, we need the following Lemmas 18, 19, and 20.

LEMMA 18. *Under the above notation and assumptions, the following* (i) *and* (ii) *hold for any $x \in k$:*

(i) $\psi'(x)=\psi(lx)$.

(ii) $\chi'(x)=\chi^f(x)$.

PROOF. (i) Since k'/k is a cyclic extension of degree l,

$$\begin{aligned}\mathrm{Tr}_{k'/\boldsymbol{F}_p}(x) &= \mathrm{Tr}_{k/\boldsymbol{F}_p}(\mathrm{Tr}_{k'/k}(x)) \\ &= \mathrm{Tr}_{k/\boldsymbol{F}_p}(lx).\end{aligned}$$

Hence by definition we have the assertion.

(ii) Since

$$\chi_{\mathfrak{p}_{n+1}}(x) \equiv x^{(N\mathfrak{p}_{n+1}-1)/l^{n+1}} \pmod{\mathfrak{p}_{n+1}}$$

and

$$\chi_{\mathfrak{p}_n}(x) \equiv x^{(N\mathfrak{p}_n-1)/l^n} \pmod{\mathfrak{p}_n},$$

we have

$$\chi_{\mathfrak{p}_{n+1}}(x) \equiv \chi_{\mathfrak{p}_n}(x)^{f'} \pmod{\mathfrak{p}_{n+1}},$$

so

$$\chi_{\mathfrak{p}_{n+1}}(x) = \chi_{\mathfrak{p}_n}(x)^{f'}, \tag{1}$$

where $f'=(N\mathfrak{p}_{n+1}-1)/(N\mathfrak{p}_n-1)l$. Next we will show

$$f' \equiv f \pmod{l^n}. \tag{2}$$

Since $N\mathfrak{p}_{n+1}=(N\mathfrak{p}_n)^l$, we have

$$f' = (1+N\mathfrak{p}_n+\cdots+(N\mathfrak{p}_n)^{l-1})/l. \tag{3}$$

Since $\zeta_{l^n} \bmod \mathfrak{p}_n \in k$ and $\zeta_{l^{n+1}} \bmod \mathfrak{p}_{n+1} \notin k$, we can write $N\mathfrak{p}_n=1+\lambda l^n$ with $\lambda \in \boldsymbol{Z}$, $\lambda \not\equiv 0 \pmod{l}$. Hence

$$(N\mathfrak{p}_n)^i \equiv 1+i\lambda l^n \pmod{l^{n+1}}$$

for $i \geqq 1$. So by (3),

$$f' \equiv \left(l+\lambda\left(\sum_{i=1}^{l-1} i\right)l^n\right)\Big/ l \pmod{l^n},$$

hence we have (2), since $\sum_{i=1}^{l-1} i$ is 0 or 1 mod l according as $l \neq 2$ or $l=2$. By (1) and (2), we have the assertion.

LEMMA 19. *Let k_0, k, and k' be as just before Lemma* 18. *Then the Galois group* $\mathrm{Gal}(k'/k_0)$ *acts on* $(k'-k)$ *faithfully.*

PROOF. Let x be any element of $k'-k$. Then $k'=k_0(x)$. In fact, since k'/k_0 is a cyclic extension of degree l^{d+1}, we see that if $k_0(x) \subsetneqq k'$, then $k_0(x) \subseteqq k$, so $x \in k$; this is a contradiction. Hence the set

$$\{x^\sigma \mid \sigma \in \mathrm{Gal}(k'/k_0)\}$$

consists of l^{d+1} different elements. This gives the assertion.

LEMMA 20. *Put*

$$B = \sum_{x \in k'-k} \chi'(x)\psi'(x).$$

Then

$$B = l^{d+1} \sum_{x \in S'} \chi'(x)\psi'(x),$$

where S is a complete representative system of $(k'-k)/\mathrm{Gal}(k'/k_0)$, *and*

$$S' = \{x \in S \mid \chi'(x) \in M\}$$
$$= \{x \in S \mid \chi'(x)^{l^{n-d}} = 1\}.$$

PROOF. By Lemma 19,

$$B = \sum_{x \in S} \Big(\sum_{\sigma \in G} \chi'(x^\sigma)\psi'(x^\sigma) \Big), \tag{1}$$

where $G = \mathrm{Gal}(k'/k_0)$. Identify G and $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{l^{n+1}})/M)$ canonically. Then

$$\psi'(x^\sigma) = \psi'(x) \quad \text{and} \quad \chi'(x^\sigma) = \chi'(x)^\sigma$$

for $\sigma \in G$, since

$$\mathfrak{p}_{n+1}^\sigma = \mathfrak{p}_{n+1} \quad \text{and} \quad \left(\frac{x}{\mathfrak{p}_{n+1}}\right)_{l^{n+1}}^\sigma = \left(\frac{x^\sigma}{\mathfrak{p}_{n+1}^\sigma}\right)_{l^{n+1}}.$$

Hence by (1),

$$B = \sum_{x \in S} \mathrm{Tr}_{\boldsymbol{Q}(\zeta_{l^{n+1}})/M}(\chi'(x))\psi'(x).$$

Since

$$\mathrm{Tr}_{\boldsymbol{Q}(\zeta_{l^n})/M}(\chi'(x)) = \begin{cases} l^{d+1}\chi'(x) & \text{if } \chi'(x) \in M, \\ 0 & \text{otherwise,} \end{cases}$$

we have the assertion.

PROOF OF THEOREM 10. Put

$$A = -\sum_{x \in k} \chi'(x)\psi'(x).$$

Then

$$g_{l^{n+1}}(\mathfrak{p}_{n+1}, a) = A - B, \tag{1}$$

where B is as in Lemma 20. By Lemma 18,

$$A = -\sum_{x \in k^\times} \chi^f(x)\psi(lx),$$

so

$$A = \chi(l)^{-f} g_{l^n}(\mathfrak{p}_n, af). \tag{2}$$

By (1), (2), and Lemma 20, we have the assertion.

Next, we will prove the following Theorem 11, which is a refinement of Theorem 10 when $l=2$ and $d=0$.

THEOREM 11. *Let the notation and assumptions be as in Theorem* 10, *and assume* $l=2$. *Then*

$$g_{2^{n+1}}(\mathfrak{p}_{n+1}, a) \equiv \left(\frac{(-1)^{2^{n-2}}2}{\mathfrak{p}_n}\right)_{2^n}^{-af} g_{2^n}(\mathfrak{p}_n, af) \pmod{2\pi_{n-d}\boldsymbol{Z}[\zeta_{2^{n-d}p}]}.$$

We can write

$$k'^{\times} = G_1' \times G_2' \text{ (direct product)}$$

and

$$k^{\times} = G_1 \times G_2 \text{ (direct product)},$$

where G_1', G_2', G_1, and G_2 are subgroups of order g', 2^{n+1}, g, and 2^n respectively,

$$g' = (N\mathfrak{p}_{n+1}-1)/2^{n+1} \not\equiv 0 \pmod 2$$

and

$$g = (N\mathfrak{p}_n-1)/2^n \not\equiv 0 \pmod 2.$$

Note that $G_i' \supset G_i$ for $i=1, 2$, since $k'^{\times}$ and $k^{\times}$ are cyclic groups. Put $e=[G_1' : G_1]=g'/g$. Then

$$e \equiv f_n \pmod{2^n} \quad \text{and} \quad e > 1$$

(cf. the proof of Lemma 18, (ii)).

For our proof of Theorem 11 we need the following

LEMMA 21. *Assume $l=2$, and let the notation and assumptions be as above. Furthermore, put*

$$T' = \{x \in k'-k \mid \chi'(x)^{2^n} = 1\}$$

and

$$C = \sum_{x \in T'} \psi'(x).$$

Then

$$C = \begin{cases} 0 & \text{if } a \text{ is even,} \\ 1-e & \text{if } a \text{ is odd.} \end{cases}$$

PROOF. If a is even, then $T'=k'-k$, so by (i) of Lemma 18,

$$\begin{aligned} C &= \sum_{x \in k'} \psi'(x) - \sum_{x \in k} \psi'(x) \\ &= \sum_{x \in k'} \psi'(x) - \sum_{x \in k} \psi(2x), \end{aligned}$$

hence

$$C = 0,$$

since

$$\sum_{x \in k'} \psi'(x) = \sum_{x \in k} \psi(2x) = \sum_{x \in k} \psi(x) = 0.$$

Next, assume a is odd. Then χ' is a surjective homomorphism from $k'^{\times}$ onto $\langle \zeta_{2^{n+1}} \rangle$ (the group generated by $\zeta_{2^{n+1}}$), so $\chi'(G_1')=\{1\}$ and $\chi'|_{G_2'}$ is an isomorphism from G_2' onto $\langle \zeta_{2^{n+1}} \rangle$. Hence $\chi'(x)^{2^n}=1$ if and only if $x \in G_1' \times G_2$. This gives

$$T' = (G_1'-G_1) \times G_2. \tag{1}$$

Let

$$G_1' = \bigcup_{i=1}^{e} g_i G_1 \quad (g_1 = 1)$$

be a coset decomposition of G_1' with respect to G_1. By (1),

(2) $$T' = \bigcup_{i=2}^{e} g_i G_1 \times G_2$$

$$= \bigcup_{i=2}^{e} g_i k^\times \text{ (disjoint union).}$$

Put $z_i = \mathrm{Tr}_{k'/k}(g_i)$ for $2 \leqq i \leqq e$. Then

(3) $$z_i \neq 0 \quad \text{for } 2 \leqq i \leqq e.$$

In fact, if we put $\zeta = \zeta_{2^{n+1}} \bmod \mathfrak{p}_{n+1}$, then we can write $g_i = \lambda + \mu\zeta$ with $\lambda, \mu \in k$. If $\lambda = 0$, then $g_i = \mu\zeta \in G_1 \times (G_2' - G_2)$; this contradicts $g_i \in G_1$. Hence $\lambda \neq 0$ and $z_i = 2\lambda \neq 0$. Since $\mathrm{Tr}_{k'/F_p}(g_i y) = \mathrm{Tr}_{k/F_p}(z_i y)$ for $y \in k^\times$, by (2) we have

$$C = \sum_{i=2}^{e} \sum_{y \in k^\times} \zeta_p^{\mathrm{Tr}_{k/F_p}(z_i y)},$$

so by (3),

$$C = (e-1) \sum_{y \in k^\times} \psi(y) = 1 - e.$$

This completes the proof.

PROOF OF THEOREM 11. If $d \geqq 1$, then $n \geqq 3$, so $(-1)^{2^{n-2}} = 1$, hence the assertion follows from Theorem 10. Hence we may assume $d = 0$, i.e., $M = \boldsymbol{Q}(\zeta_{2^n})$. For simplicity, put $I = 2\pi_n \boldsymbol{Z}[\zeta_{2^n p}]$. By Lemma 20,

$$B = 2 \sum_{x \in S'} \chi'(x)\psi'(x)$$

$$\equiv 2 \sum_{x \in S'} \psi'(x) \pmod{I},$$

so

$$B \equiv C \pmod{I},$$

since $k' - k = S \cup S^\sigma$ (disjoint union) and $\psi'(x^\sigma) = \psi'(x)$ for a generator σ of $\mathrm{Gal}(k'/k)$. Hence by (1) in the proof of Theorem 10, we have

(1) $$g_{2^{n+1}}(\mathfrak{p}_{n+1}, a) - A \equiv -C \pmod{I}.$$

If a is even, then

$$\left(\frac{(-1)^{2^{n-2}}}{\mathfrak{p}_n}\right)_{2^n}^{a} = 1 \quad \text{and} \quad C = 0$$

by Lemma 21, so (1) gives the assertion. Now assume a is odd. Then by (1) we have

$$(2) \qquad g_{2^{n+1}}(\mathfrak{p}_{n+1}, a)-A \equiv \begin{cases} 0 \pmod{I} & \text{if } n \geqq 3, \\ 2 \pmod{I} & \text{if } n = 2, \end{cases}$$

since by Lemma 21,

$$C = 1-e \equiv \begin{cases} 0 \pmod 4 & \text{if } n \geqq 3, \\ 2 \pmod 4 & \text{if } n = 2. \end{cases}$$

Since $A \equiv 1 \pmod{\pi_n \boldsymbol{Z}[\zeta_{2^n p}]}$, we have $2(A+1) \equiv 0 \pmod I$, so $A+2 \equiv -A \pmod I$. Hence (2) implies

$$g_{2^{n+1}}(\mathfrak{p}_{n+1}, a) \equiv \begin{cases} A \pmod I & \text{if } n \geqq 3, \\ -A \pmod I & \text{if } n = 2. \end{cases}$$

Since $(-1/\mathfrak{p}_n)_{2^n} = -1$ and af is odd, this gives the assertion.

LEMMA 22. *For any prime number l, three congruences* (i)$\sim$(iii) *in Lemma* 3 *of* [**13**] *and the following congruence* (iv) *hold* mod $l\pi_n$.

(iv) $J_{l^n}^{(a)}(\mathfrak{a})^l \equiv J_{l^n}^{(la)}(\mathfrak{a}) \pmod{l\pi_n}$ *if* $a=(a_1, \cdots, a_r) \not\equiv (0, \cdots, 0) \pmod{l^n}$.

PROOF. Since the congruences (ii)$\sim$(iv) follow directly from (i) and (1) of [**13**], § 1, it suffices to prove (i) for $j=1$ by induction on j. By definition,

$$g_{l^n}(\mathfrak{p}, a) = -\sum_x \chi_{\mathfrak{p}}^a(x)\phi_{\mathfrak{p}}(x),$$

so putting $A = -\sum_{x \neq 0}(\chi_{\mathfrak{p}}^a(x)-1)\phi_{\mathfrak{p}}(x)$, we have

$$(1) \qquad g_{l^n}(\mathfrak{p}, a) = 1+A.$$

By taking the l-th power of both sides of (1),

$$g_{l^n}(\mathfrak{p}, a)^l = 1+A^l+\sum_{i=1}^{l-1}\binom{l}{i}A^i,$$

so

$$(2) \qquad g_{l^n}(\mathfrak{p}, a)^l \equiv 1+A^l \pmod{l\pi_n},$$

since $\binom{l}{i} \equiv 0 \pmod l$, $\chi_{\mathfrak{p}}^a(x)-1 \equiv 0 \pmod{\pi_n}$, and $A \equiv 0 \pmod{\pi_n}$. By putting $X_x = (\chi_{\mathfrak{p}}^a(x)-1)\phi_{\mathfrak{p}}(x)$ in the identity as polynomials

$$\Big(\sum_{x \neq 0} X_x\Big)^l = \sum_{x \neq 0} X_x^l + lf(X)$$

with some $f(X) \in \boldsymbol{Z}[X]$ without constant term, we have

$$(3) \qquad A^l \equiv (-1)^l \sum_{x \neq 0}(\chi_{\mathfrak{p}}^a(x)-1)^l \phi_{\mathfrak{p}}(lx) \pmod{l\pi_n}.$$

Since

$$(X-1)^l = X^l+(-1)^l+\sum_{i=1}^{l-1}\binom{l}{i}X^i(-1)^{l-i}$$

and

$$\binom{l}{i} \equiv (-1)^{i-1}l/i \pmod{l^2},$$

we have the congruence in the polynomial ring $\boldsymbol{Z}[X]$:

$$(X-1)^l \equiv X^l+(-1)^l+l(-1)^{l-1}\sum_{i=1}^{l-1}X^i/i \pmod{l^2\boldsymbol{Z}[X]}.$$

Putting $X=\chi_{\mathfrak{p}}^a(x)$ and using $\chi_{\mathfrak{p}}^a(x)\equiv 1 \pmod{\pi_n}$, we have

$$\begin{aligned}(\chi_{\mathfrak{p}}^a(x)-1)^l &\equiv \chi_{\mathfrak{p}}^{al}(x)+(-1)^l+l(-1)^{l-1}\sum_{i=1}^{l-1}\frac{1}{i} \pmod{l\pi_n}\\ &\equiv \chi_{\mathfrak{p}}^{al}(x)+(-1)^l+l(-1)^{l-1}\delta \pmod{l\pi_n},\end{aligned}$$

where $\delta=0$ or 1 according as $l\neq 2$ or $l=2$. Using this and (3),

$$A^l \equiv (-1)^{l-1}\chi_{\mathfrak{p}}^{al}(l)^{-1}g_{ln}(\mathfrak{p}, al)-1+l\delta \pmod{l\pi_n},$$

since

$$\sum_{x\neq 0}\psi_{\mathfrak{p}}(lx) = -1$$

and

$$\sum_{x\neq 0}\chi_{\mathfrak{p}}^{al}(x)\psi_{\mathfrak{p}}(lx) = -\chi_{\mathfrak{p}}^{al}(l)^{-1}g_{ln}(\mathfrak{p}, al).$$

Hence by (2),

$$g_{ln}(\mathfrak{p}, a)^l \equiv (-1)^{l-1}\chi_{\mathfrak{p}}^{al}(l)^{-1}g_{ln}(\mathfrak{p}, al)+l\delta \pmod{l\pi_n}.$$

If $l\neq 2$, then this implies the desired congruence. If $l=2$, then this implies

$$\begin{aligned}g_{ln}(\mathfrak{p}, a)^l &\equiv -\chi_{\mathfrak{p}}^{al}(l)^{-1}g_{ln}(\mathfrak{p}, al)+2 \pmod{l\pi_n}\\ &\equiv \chi_{\mathfrak{p}}^{al}(l)^{-1}g_{ln}(\mathfrak{p}, al) \pmod{l\pi_n},\end{aligned}$$

since

$$2 \equiv 2\chi_{\mathfrak{p}}^{al}(l)^{-1}g_{ln}(\mathfrak{p}, al) \pmod{l\pi_n}.$$

This completes the proof.

LEMMA 23. *For any prime number l and any fractional ideal $\mathfrak{a}$ of $\boldsymbol{Q}(\zeta_{l^{n+1}})$ which is prime to l, the following* (i) *and* (ii) *hold.*

(i) $g_{l^{n+1}}(\mathfrak{a}, al)=g_{ln}(N_{n+1,n}(\mathfrak{a}), a)$ *for any* $a\in\boldsymbol{Z}$.

(ii) $J_{l^{n+1}}^{(al)}(\mathfrak{a})=J_{l^n}^{(a)}(N_{n+1,n}(\mathfrak{a}))$ *if* $a=(a_1, \cdots, a_r)\not\equiv(0, \cdots, 0) \pmod{l^n}$.

PROOF. By a well-known relation between Gauss sums and Jacobi sums (cf. e.g., (1) in [**13**], § 1), it suffices to prove only (i) when $\mathfrak{a}=\mathfrak{p}_{n+1}$ is a prime ideal of $\boldsymbol{Q}(\zeta_{l^{n+1}})$. Put $\boldsymbol{F}_i=\boldsymbol{Z}[\zeta_{li}]/\mathfrak{p}_i$ for $i=n$, $n+1$, where $\mathfrak{p}_n=\mathfrak{p}_{n+1}\cap\boldsymbol{Q}(\zeta_{l^n})$. If

$\mathfrak{p}_n$ decomposes in $\boldsymbol{Q}(\zeta_{l^{n+1}})/\boldsymbol{Q}(\zeta_{l^n})$, then $N_{n+1,n}(\mathfrak{p}_{n+1})=\mathfrak{p}_n$, $\boldsymbol{F}_{n+1}=\boldsymbol{F}_n$, and $\chi_{\mathfrak{p}_{n+1}}^{l}=\chi_{\mathfrak{p}_n}$, so by the definition of Gauss sums we have (i). Now assume that $\mathfrak{p}_n$ does not decompose in $\boldsymbol{Q}(\zeta_{l^{n+1}})/\boldsymbol{Q}(\zeta_{l^n})$. Since $N\mathfrak{p}_{n+1}=(N\mathfrak{p}_n)^l$, we have

$$(1+N\mathfrak{p}_n+\cdots+N\mathfrak{p}_n^{l-1})(N\mathfrak{p}_n-1)/l^n=(N\mathfrak{p}_{n+1}-1)/l^n,$$

so

$$x^{(N\mathfrak{p}_{n+1}-1)/l^n}=N_{\boldsymbol{F}_{n+1}/\boldsymbol{F}_n}(x)^{(N\mathfrak{p}_n-1)/l^n},$$

i.e.,

$$\chi_{\mathfrak{p}_{n+1}}^{l}(x)=\chi_{\mathfrak{p}_n}\circ N_{\boldsymbol{F}_{n+1}/\boldsymbol{F}_n}(x)$$

for $x\in\boldsymbol{F}_{n+1}$. Hence by a relation of Davenport-Hasse (cf. e.g., [**17**], Exercise 6.4),

$$g_{l^{n+1}}(\mathfrak{p}_{n+1},\ a\boldsymbol{l})=g_{l^n}(\mathfrak{p}_n,\ a)^l.$$

This gives the assertion.

THEOREM 12. *Assume* $l=2$ *and* $a=(a_1,\cdots,a_r)\not\equiv(0,\cdots,0)\pmod{2^n}$. *Then*

$$J_{2^{n+1}}^{(a)}(\mathfrak{a})\equiv J_{2^n}^{(a)}(\mathfrak{a})\pmod{2\pi_n}$$

for any fractional ideal $\mathfrak{a}$ *of* $\boldsymbol{Q}(\zeta_{l^n})$ *prime to* 2.

PROOF. Since $J_{2^{n+1}}^{(a)}(\mathfrak{a})^\sigma=J_{2^{n+1}}^{(a)}(\mathfrak{a}^\sigma)=J_{2^{n+1}}^{(a)}(\mathfrak{a})$ for the generator σ of $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{2^{n+1}})/\boldsymbol{Q}(\zeta_{2^n}))$, we have $J_{2^{n+1}}^{(a)}(\mathfrak{a})\in\boldsymbol{Q}(\zeta_{2^n})$. Hence it suffices to prove the congruence mod $2\pi_{n+1}$. We may assume that $\mathfrak{a}=\mathfrak{p}_n$ is a prime ideal of $\boldsymbol{Q}(\zeta_{l^n})$. Let $\mathfrak{p}_{n+1}$ be a prime ideal of $\boldsymbol{Q}(\zeta_{l^{n+1}})$ lying above $\mathfrak{p}_n$. By Hasse's congruence ([**5**], p. 61; see also [**11**], Theorem 2),

$$J_{2^{n+1}}^{(a)}(\mathfrak{p}_{n+1})\equiv 1\pmod{\pi_{n+1}^2},$$

so

$$(1)\qquad J_{2^{n+1}}^{(a)}(\mathfrak{p}_{n+1})^\sigma\equiv J_{2^{n+1}}^{(a)}(\mathfrak{p}_{n+1})\pmod{2\pi_{n+1}},$$

since

$$(\pi_{n+1}^i)^\sigma\equiv\pi_{n+1}^i\pmod{2\pi_{n+1}}$$

for $i\geqq 2$. First, assume that $\mathfrak{p}_n$ decomposes in $\boldsymbol{Q}(\zeta_{2^{n+1}})/\boldsymbol{Q}(\zeta_{2^n})$. Then $N_{n+1,n}(\mathfrak{p}_{n+1})=\mathfrak{p}_n$. Hence by (1),

$$\begin{aligned}J_{2^{n+1}}^{(a)}(\mathfrak{p}_n)&=J_{2^{n+1}}^{(a)}(\mathfrak{p}_{n+1}\cdot\mathfrak{p}_{n+1}^\sigma)\\&=J_{2^{n+1}}^{(a)}(\mathfrak{p}_{n+1})\cdot J_{2^{n+1}}^{(a)}(\mathfrak{p}_{n+1})^\sigma\\&\equiv J_{2^{n+1}}^{(a)}(\mathfrak{p}_{n+1})^2\pmod{2\pi_{n+1}},\end{aligned}$$

so by Lemma 22,

$$J_{2^{n+1}}^{(a)}(\mathfrak{p}_n)\equiv J_{2^{n+1}}^{(2a)}(\mathfrak{p}_{n+1})\pmod{2\pi_{n+1}},$$

hence by (ii) of Lemma 23 we have the assertion. Now assume that $\mathfrak{p}_n$ does

not decompose in $\boldsymbol{Q}(\zeta_{2^{n+1}})/\boldsymbol{Q}(\zeta_{2^n})$. By Theorem 11 and a well-known relation between Gauss sums and Jacobi sums,

$$(2) \qquad J_{2^{n+1}}^{(a)}(\mathfrak{p}_{n+1}) \equiv J_{2^n}^{(af)}(\mathfrak{p}_n) \pmod{2\pi_{n+1}}.$$

Since the right side is equal to $J_{2^n}^{(a)}(\mathfrak{p}_n)^{\sigma_f}$, by (1) (replacing $n+1$ by n) we have

$$J_{2^{n+1}}^{(a)}(\mathfrak{p}_{n+1}) \equiv J_{2^n}^{(a)}(\mathfrak{p}_n) \pmod{2\pi_{n+1}}.$$

This completes the proof.

REMARK. (1) In the above proof, we used Lemma 23 when $\mathfrak{p}_n$ decomposes in $\boldsymbol{Q}(\zeta_{2^{n+1}})/\boldsymbol{Q}(\zeta_{2^n})$, so we did not use the Davenport-Hasse relation for our proof of Theorem 12.

(2) In the above proof, we can use Theorem 10 and (iii) of Lemma 22 in place of Theorem 11. In fact, by Theorem 10,

$$g_{2^{n+1}}(\mathfrak{p}_{n+1}) \equiv \chi_{\mathfrak{p}_n}(2)^{-f} g_{2^n}(\mathfrak{p}_n)^{\sigma_f} \pmod{2}.$$

Making ω in (iii) of Lemma 22 operate on both sides,

$$g_{2^{n+1}}(\mathfrak{p}_{n+1})^{\omega} \equiv (g_{2^n}(\mathfrak{p}_n)^{\omega})^{\sigma_f} \pmod{2\pi_{n+1}},$$

since $(1+2)^{\omega} \equiv (-1)^{\omega} \equiv 1 \pmod 4$. By (iii) of Lemma 22 and (ii) of Lemma 18, we have (2) in the proof of Theorem 12.

THEOREM 13. *Assume* $l=2$ *and* $a=(a_1, \cdots, a_r) \not\equiv (0, \cdots, 0) \pmod{2^n}$. *Let* $\mathfrak{a}$ *be a fractional ideal of* $\boldsymbol{Q}(\zeta_{2^n})$ *prime to* 2, *and let* r'' *be a half of the number of* i $(0 \leqq i \leqq r)$ *such that* $a_i \not\equiv 0 \pmod 2$, *where* $a_0 = -\sum_{i=1}^{r} a_i$. *Then*

$$\begin{aligned} N\mathfrak{a} \cdot J_{2^n}^{(a)}(\mathfrak{a}) &\equiv 1 + r'' \langle 2, \mathfrak{a} \rangle_{2^n} \pi_n^2 \pmod{\pi_n^3} \\ &\equiv 1 + r'' \cdot \frac{(N\mathfrak{a})^2 - 1}{8} \pi_n^2 \pmod{\pi_n^3} \\ &\equiv \begin{cases} 1 + r'' \cdot \dfrac{(N\mathfrak{a})^2 - 1}{2} \pmod 8 & \text{if } n = 1, \\ 1 + r'' \cdot \dfrac{N\mathfrak{a} - 1}{2} \pmod{\pi_n^3} & \text{if } n = 2, \\ 1 \pmod{\pi_n^3} & \text{if } n \geqq 3. \end{cases} \end{aligned}$$

PROOF. We may assume that $\mathfrak{a} = \mathfrak{p}$ is a prime ideal of $\boldsymbol{Q}(\zeta_{l^n})$. Put $\chi_{\mathfrak{p}} = \chi$, $\psi_{\mathfrak{p}} = \psi$, and $\lambda(x) = \langle x, \mathfrak{p} \rangle_{2^n}$ for simplicity. Then by definition,

$$\chi(x) = \zeta_{2^n}^{\lambda(x)} = (1 - \pi_n)^{\lambda(x)}$$

for $x \in (\boldsymbol{Z}[\zeta_{2^n}]/\mathfrak{p})^{\times}$. Hence for $b \in \boldsymbol{Z}$,

$$g_{2^n}(\mathfrak{p}, b) = -\sum_{x \in Z[\zeta_{2^n}]/\mathfrak{p}} \chi^b(x)\psi(x)$$
$$= -\sum_{x \neq 0}(1-\pi_n)^{\lambda(x)b}\psi(x)$$
$$\equiv 1+bc\pi_n+d\pi_n^2 \pmod{\pi_n^3},$$

where

$$c = \sum_{x \neq 0}\lambda(x)\psi(x),$$
$$c' = -\sum_{x \neq 0}\lambda(x)^2\psi(x),$$

and

$$d = -\sum_{x \neq 0}\frac{\lambda(x)b(\lambda(x)b-1)}{2}\psi(x)$$
$$= (b^2c'+bc)/2.$$

Since $\sum_{i=0}^{r} a_i = 0$,

$$\sum_{i=0}^{r} a_i^2 = -2\sum_{i<j}^{r} a_i a_j.$$

Hence

$$N\mathfrak{p}\cdot J_{2^n}^{(\mathfrak{a})}(\mathfrak{p}) = \prod_{j=0}^{r} g_{2^n}(\mathfrak{p}, a_i)$$
$$\equiv 1+\left(c^2\sum_{i<j} a_i a_j + \frac{c'}{2}\sum_{i=0}^{r} a_i^2\right)\pi_n^2 \pmod{\pi_n^3}$$
$$\equiv 1+(c^2-c')\left(\sum_{i<j} a_i a_j\right)\pi_n^2 \pmod{\pi_n^3}.$$

Since

$$\sum_{i<j} a_i a_j \equiv r'' \pmod 2$$

and

$$c^2-c \equiv \lambda(2) \pmod 2$$

by [**11**], Lemma 7, we have the first congruence. Since

$$\langle 2, \mathfrak{a}\rangle_{2^n} \equiv \langle 2, N\mathfrak{a}\rangle_2$$
$$\equiv (N\mathfrak{a}^2-1)/8 \pmod 2,$$

we have the second one. If $n \geqq 2$, then $N\mathfrak{a} \equiv 1 \pmod 4$, so

$$(N\mathfrak{a}^2-1)/8 \equiv (N\mathfrak{a}-1)/4 \pmod 2.$$

If $n \geqq 3$, then $N\mathfrak{a} \equiv 1 \pmod 8$. This gives the assertion.

REMARK. The above Theorem 13 is a generalization of Ihara [**6**], Corollary to Theorem 7 (he deals with the case $r=2$ and $(a_0, a_1, a_2, 2)=1$ by a different method).

THEOREM 14. *Assume* $l=2$ *and* $a=(a_1, \cdots, a_r) \not\equiv (0, \cdots, 0) \pmod{2^n}$. *Let* $\eta \in \boldsymbol{Q}(\zeta_4)^\times$ *be such that* $\nu_2(\eta-1)=3$, *where* ν_2 *is the normalized additive valuation of* $\boldsymbol{Q}_2(\zeta_4)$. *Then*

$$J_{2^n}^{(a)}((\eta)) \equiv (-1)^{r''} \pmod{2\pi_n},$$

where r'' *is as in Theorem* 13.

PROOF. By Theorem 12, we may suppose $n=2$. Since $\nu_2(\eta-1)=3$ and $\boldsymbol{Q}(\zeta_4)$ is totally imaginary,

$$N((\eta)) = N_2(\eta) \equiv 1+4 \pmod 8,$$

so by Theorem 13,

$$\begin{aligned} J_{2^n}^{(a)}((\eta)) &\equiv 1+2r'' \pmod{2\pi_n} \\ &\equiv (-1)^{r''} \pmod{2\pi_n}. \end{aligned}$$

This completes the proof.

THEOREM 15. *Let the notation and assumptions be as in Theorem* 14. *Then*

$$i_{2^n}^{(a)}(\eta) \equiv 2^{n-1}r'' \pmod{2^n}.$$

PROOF. By Weil [**18**],

$$J_{2^n}^{(a)}((\eta)) = \zeta_{2^n}^{i(\eta)} \eta^{\omega_n(a)} \quad \text{with} \quad i(\eta) = i_{2^n}^{(a)}(\eta) \in \boldsymbol{Z}/2^n\boldsymbol{Z}$$

(see the formula (*) just before Theorem 3 of [**13**]). Since $\eta \equiv 1 \pmod{2\pi_2}$,

$$J_{2^n}^{(a)}((\eta)) \equiv \zeta_{2^n}^{i(\eta)} \pmod{2\pi_2},$$

so by Theorem 14,

$$\zeta_{2^n}^{i(\eta)} \equiv \zeta_{2^n}^{2^{n-1}r''} \pmod{2\pi_n}.$$

This gives the assertion.

ACKNOWLEDGEMENTS. This work was done during my stay 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 encouragements 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. Tamagawa, 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. I wish to thank the Department of Mathematics, the Graduate Center of CUNY, MSRI, and the University of Minnesota for their hospitality. Finally, I wish to thank the referee to correct an error in the proof of Theorem 1 of [**14**].

References

[1] E. Artin and H. Hasse, Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln, Abh. Math. Sem. Univ. Hamburg, **6** (1928), 146-162.

[2] R. Coleman and W. McCallum, Stable reduction of Fermat curves and Jacobi sum Hecke characters, J. Reine Angew. Math., **385** (1988), 41-101.

[3] R. Coleman, Anderson-Ihara theory: Gauss sums and circular units, Adv. Stud. Pure Math., **17** (1989), 55-72.

[4] H. Hasse, Normenresttheorie galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante abelscher Zahlkörper, J. Fac. Sci. Univ. Tokyo, **2** (1934), 477-498.

[5] H. Hasse, Zetafunktionen und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus, Abh. Deut. Akad. Wiss. Berlin Kl. Math. Nat., 1954, n° **4** (1955), 70 pages.

[6] Y. Ihara, Profinite braid groups, Galois representations and complex multiplications, Ann. of Math., **123** (1986), 43-106.

[7] K. Iwasawa, On explicit formulas for the norm residue symbol, J. Math. Soc. Japan, **20** (1968), 151-165.

[8] K. Iwasawa, Lectures on p-adic L-functions, Ann. of Math. Stud., **74**, Princeton University Press, 1972.

[9] A. Kudo, On Iwasawa's explicit formula for the norm residue symbol, Mem. Fac. Sci. Kyushu Univ., **26** (1971), 139-148.

[10] E. Maus, Arithmetisch disjunkte Körper, J. Reine Angew. Math., **226** (1967), 184-203.

[11] H. Miki, On the l-adic expansion of certain Gauss sums and its applications, Adv. Stud. Pure Math., **12** (1987), 87-118.

[12] H. Miki, On the conductor of the Jacobi sum Hecke character, Preprint, April 1988, 10 pages (unpublished): talk at the Number Theory Seminar (Goldfeld), Columbia Univ., Mar. 21, 1988.

[13] H. Miki, On the conductor of the Jacobi sum Hecke character, Compositio Math., **92** (1994), 23-41.

[14] H. Miki, On the calculation of certain Hilbert norm residue symbols and its application, J. Number Theory, **50** (1995), 87-105.

[15] D. Rohrlich, Jacobi sums and explicit reciprocity laws, Compositio Math., **60** (1986), 97-114.

[16] J.-P. Serre, Corps locaux, 2nd ed., Hermann, Paris, 1968, (English translation), Local Fields, GTM **67**, Springer, New York-Berlin-Heidelberg, 1979.

[17] L. Washington, Introduction to cyclotomic fields, GTM **83**, Springer, Berlin-Heidelberg-New York, 1982.

[18] A. Weil, Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc., **73** (1952), 487-495.

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
Kyoto 606
Japan